



Уральский государственный юридический университет
Проект "CrimLib.info"

Союз криминалистов и криминологов
Проект "Ритвус"

ТЕХНОЛОГИИ XXI ВЕКА В ЮРИСПРУДЕНЦИИ

3.0

Материалы Третьей международной
научно-практической конференции



г. Екатеринбург

21 мая 2021 г.

ФГБОУ ВО
«Уральский государственный юридический университет»
Проект «CrimLib.info»
Союз криминалистов и криминологов
Проект «Ритвус»

ТЕХНОЛОГИИ ХХІ ВЕКА В ЮРИСПРУДЕНЦИИ

**Материалы
Международной научно-практической конференции
(Екатеринбург, 21 мая 2021 года)**



Екатеринбург
2021

УДК 34
ББК 67
Т38

Рецензенты:

А. А. Каминский, доктор юридических наук, профессор, заведующий кафедрой криминалистики и судебных экспертиз Удмуртского государственного университета

А. А. Беляков, доктор юридических наук, профессор, заведующий кафедрой криминалистики Уральского государственного юридического университета

Ответственный редактор:

Д. В. Бахтеев, кандидат юридических наук, доцент, доцент кафедры криминалистики Уральского государственного юридического университета

Т38 Технологии XXI века в юриспруденции: материалы Третьей международной научно-практической конференции (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. — Екатеринбург: Уральский государственный юридический университет. — 2021. — 523 с.

ISBN 978-5-7845-0651-1

В сборнике представлены статьи учёных-юристов, представителей юридической практики и начинающих исследователей, принявших участие в Третьей международной научно-практической конференции «Технологии XXI века в юриспруденции», посвящённой отдельным проблемам юридических науки и практики, связанным с современными технологиями.

УДК 34
ББК 67

Конференция была организована при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта 18-29-16001 «Комплексное исследование правовых, криминалистических и этических аспектов, связанных с разработкой и функционированием систем искусственного интеллекта».

ISBN 978-5-7845-0651-1

© Авторы, 2021.
© Уральский государственный
юридический университет, 2021.

СОДЕРЖАНИЕ

Раздел I

ОБЩИЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ И ЮРИДИЧЕСКОМ ОБРАЗОВАНИИ

Кодан Сергей Владимирович

ЭЛЕКТРОННЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ В ИЗУЧЕНИИ ИСТОРИИ
ПОЛИТИЧЕСКИХ И ПРАВОВЫХ УЧЕНИЙ..... 13

Бахтеев Дмитрий Валерьевич, Максимова Анастасия Валерьевна

ТЕХНОЛОГИЯ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ КАК ПОТЕНЦИАЛЬНЫЙ
МЕТОД В ПРЕПОДАВАНИИ КРИМИНАЛИСТИКИ И ИЗУЧЕНИИ
КРИМИНАЛИСТИЧЕСКИХ ОБЪЕКТОВ..... 23

Каменев Александр Сергеевич

ТРАНСФОРМАЦИЯ ФУНКЦИИ ЗАЩИТЫ В УГОЛОВНОМ
СУДОПРОИЗВОДСТВЕ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ..... 31

Колесникова Наталья Сергеевна

ПРОБЛЕМА ДОСТОВЕРНОСТИ ЗАКЛЮЧЕНИЯ СУДЕБНОГО ЭКСПЕРТА 39

Шашкова Ирина Алексеевна

ОСНОВНЫЕ НАПРАВЛЕНИЯ РЕГУЛИРОВАНИЯ ЗАЩИТЫ
ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВОЙ
ТРАНСФОРМАЦИИ ОБЩЕСТВЕННЫХ ОТНОШЕНИЙ..... 43

Адалина Алина Александровна

СОВРЕМЕННОЕ ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ФИНАНСОВО-
ЭКОНОМИЧЕСКОЙ ЭКСПЕРТИЗЫ..... 50

Кириленко Анна Сергеевна, Сахипова Сауле Ассаматовна

ПРАВОВОЕ ОБЕСЕПЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В
РОССИЙСКОЙ ФЕДЕРАЦИИ..... 57

Чепурнов Вадим Александрович

РЕГУЛЯТОРНЫЕ «ПЕСОЧНИЦЫ» НА ТЕРРИТОРИИ РОССИЙСКОЙ
ФЕДЕРАЦИИ: ПРАВОВАЯ РЕГЛАМЕНТАЦИЯ И ПЕРСПЕКТИВЫ
ПРИМЕНЕНИЯ В ОТЕЧЕСТВЕННОМ ПРАВЕ..... 63

Раздел II

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ, ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ, РОБОТОТЕХНИКА

Реховский Александр Фёдорович

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УГОЛОВНОМ
ПРОЦЕССЕ КИТАЯ 69

Бахтеев Дмитрий Валерьевич

ОНТОЛОГИЧЕСКИЕ ОСНОВЫ РАЗРАБОТКИ ИНТЕЛЛЕКТУАЛЬНОЙ
СИСТЕМЫ АНАЛИЗА, ПРОГНОЗИРОВАНИЯ И ПРЕДУПРЕЖДЕНИЯ
РИСКОВ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ..... 78

Евстратова Юлиана Айратовна

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО
ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ
РОССИЙСКОЙ ФЕДЕРАЦИИ 87

Зазулин Анатолий Игоревич

ОЦЕНКА ДОКАЗАТЕЛЬСТВ, ПОЛУЧЕННЫХ В РЕЗУЛЬТАТЕ
ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА 94

Коваленко Ксения Евгеньевна, Коваленко Наталья Евгеньевна

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ИЛИ ОТОБРАЖЕНИЕ ЗАПРОСА
ОБЩЕСТВА И ПРАВА 104

Шарапа Инга Александровна

АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ К РЕГУЛИРОВАНИЮ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА 111

Тарасова Людмила Валерьевна

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В
КРИМИНАЛИСТИЧЕСКОМ ИССЛЕДОВАНИИ ПОДПИСЕЙ 116

Салтыкова Алёна Евгеньевна

ЮРИДИЧЕСКИЕ АСПЕКТЫ, СВЯЗАННЫЕ С ОБЩЕСТВЕННО ОПАСНЫМИ
ПОСЛЕДСТВИЯМИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА 122

Раздел III

РАСПРЕДЕЛЁННЫЙ РЕЕСТР, СМАРТ-КОНТРАКТЫ, КРИПТОВАЛЮТЫ И ИНЫЕ ЦИФРОВЫЕ ПРОДУКТЫ

Олифиренко Екатерина Павловна

ИСПОЛЬЗОВАНИЕ КРИПТОВАЛЮТЫ В ПРОТИВОПРАВНОЙ
ДЕЯТЕЛЬНОСТИ: ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ 129

Можаева Людмила Евгеньевна, Савченко Дмитрий Геннадьевич

КРИПТОВАЛЮТА В РЕСПУБЛИКЕ БЕЛАРУСЬ: ПРОБЛЕМЫ И ПУТИ ИХ
РЕШЕНИЯ 138

Ржанникова Светлана Сергеевна, Лобанов Руслан Эльмирович

НЕКОТОРЫЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБОРОТА
КРИПТОВАЛЮТЫ..... 143

Гридасов Владислав Денисович

ИЗМЕНЕНИЕ ПРАВОВОГО РЕЖИМА КРИПТОВАЛЮТЫ В РОССИИ НА
ОСНОВЕ ЗАРУБЕЖНОГО ОПЫТА 148

Гурьева Екатерина Евгеньевна

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ «БЛОКЧЕЙН» В ИЗБИРАТЕЛЬНОМ
ПРОЦЕССЕ..... 157

Гусейнов Рамиль Гахраманович, Стренин Данил Алексеевич,

Курилюк Юлия Евгеньевна

ЦИФРОВЫЕ ПЛАТФОРМЫ КАК МЕХАНИЗМ ОБЕСПЕЧЕНИЯ РОСТА
ЦИФРОВОЙ ЭКОНОМИКИ РОССИИ..... 168

Мелентьева Валерия Валерьевна

РАЗВИТИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ КРИПТОВАЛЮТЫ: ОПЫТ
РОССИИ И ЗАРУБЕЖНЫХ СТРАН..... 172

Шандарович Игорь Олегович, Кислицкая Надежда Александровна

ИДЕНТИФИКАЦИЯ БИТКОИН-АДРЕСОВ И ПОДОЗРЕВАЕМЫХ, ИЗЪЯТИЕ
БИТКОИНОВ С КОШЕЛЬКОВ ПОДОЗРЕВАЕМЫХ 180

Раздел IV

ГЕНОМНЫЕ ИССЛЕДОВАНИЯ, РЕПРОДУКТИВНЫЕ ТЕХНОЛОГИИ

Кручинина Надежда Валентиновна

РОЛЬ НАУКИ В ЗАЩИТЕ ОТ КРИМИНАЛЬНЫХ РИСКОВ
ВСПОМОГАТЕЛЬНЫХ РЕПРОДУКТИВНЫХ ТЕХНОЛОГИЙ 188

Бородин Сергей Сергеевич

РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ ПО ИСПОЛЬЗОВАНИЮ РЕЗУЛЬТАТОВ
ГЕНЕТИЧЕСКИХ ИССЛЕДОВАНИЙ ПРИ СОГЛАСОВАНИИ УСЛОВИЙ
ДОГОВОРОВ 192

Попов Вадим Петрович

ФАЛЬСИФИКАЦИЯ ГЕНЕТИЧЕСКИХ МАТЕРИАЛОВ:
КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ 198

Юдин Егор Витальевич

СОЦИАЛЬНАЯ ЗНАЧИМОСТЬ ГЕНЕТИЧЕСКИХ ТЕХНОЛОГИЙ И ИХ
ИСПОЛЬЗОВАНИЯ В МЕДИЦИНСКИХ ЦЕЛЯХ: ВЫЗОВ
СУЩЕСТВУЮЩЕМУ ОТЕЧЕСТВЕННОМУ ПРАВОВОМУ
РЕГУЛИРОВАНИЮ 203

Раздел V

ИНТЕРНЕТ, СОЦИАЛЬНЫЕ СЕТИ

Щелконогова Елена Владимировна

УГОЛОВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРАВООТНОШЕНИЙ,
ВОЗНИКАЮЩИХ В СЕТИ ИНТЕРНЕТ 211

Очеретько Елена Александровна

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПУБЛИЧНОГО
ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ, СОЦИАЛЬНЫХ СЕТЕЙ И
МЕДИАРЕСУРСОВ 218

Анисимова Алина Сергеевна

К ВОПРОСУ О ПРАВОВОМ РЕГУЛИРОВАНИИ СЕТИ ИНТЕРНЕТ: РЕАЛИИ
21 ВЕКА 224

Анисимова Алина Сергеевна

ТЕХНИКО-ПРАВОВЫЕ НОРМЫ РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ В СЕТИ
ИНТЕРНЕТ 230

Жиляева Александра Михайловна

НЕКОТОРЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ В СЕТИ
ИНТЕРНЕТ 236

Богатырева Софья Викторовна

ПРОБЛЕМЫ РАСКРЫТИЯ МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ С
ИСПОЛЬЗОВАНИЕМ ФИШИНГОВЫХ САЙТОВ И ПУТИ ИХ РЕШЕНИЯ. 241

Судариков Дмитрий Николаевич

ПРОБЛЕМЫ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА
ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ В БОРЬБЕ С ЭКСТРЕМИЗМОМ И
ПУТИ ИХ РЕШЕНИЯ 246

Раздел VI

ЭЛЕКТРОННОЕ ПРАВОСУДИЕ, ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Бурдина Елена Владимировна

ЦИФРОВИЗАЦИЯ СУДОВ И СПРАВЕДЛИВОСТЬ СУДЕБНОГО
РАЗБИРАТЕЛЬСТВА: В ПОИСКАХ БАЛАНСА 254

Кукеев Аскар Кульчимбаевич

КОНСТИТУЦИОННО-ПРАВОВЫЕ ОСНОВЫ ОРГАНИЗАЦИИ
ЭЛЕКТРОННОГО СУДОПРОИЗВОДСТВА В РЕСПУБЛИКЕ КАЗАХСТАН 262

Белошицкая Екатерина Вячеславовна

ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ В СУДАХ ОБЩЕЙ ЮРИСДИКЦИИ
..... 273

Хасан Самер Хажар

НОРМАТИВНАЯ ЗАКОНОДАТЕЛЬНАЯ БАЗА, РЕГЛАМЕНТИРУЮЩАЯ
ОКАЗАНИЕ ГОСУДАРСТВЕННЫХ УСЛУГ 279

Буряков Кирилл Константинович

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ПРИНЦИПА ДИСПОЗИТИВНОСТИ ПРИ
РАССМОТРЕНИИ ДЕЛ СУДАМИ ОБЩЕЙ ЮРИСДИКЦИИ С
ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ 283

Гриднев Владимир Сергеевич, Рословец Кристина Сергеевна	
ПЕРСПЕКТИВЫ РАЗВИТИЯ НАЛОГОВОГО МОНИТОРИНГА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ.....	288

Загребин Даниил Геннадьевич	
ЭЛЕКТРОННОЕ ПРАВОСУДИЕ В РОССИИ: ПРОБЛЕМНЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ.....	292

Зверева Екатерина Дмитриевна	
ЦИФРОВИЗАЦИЯ СИСТЕМЫ ИСПОЛНИТЕЛЬНОГО ПРОИЗВОДСТВА В РОССИЙСКОЙ ФЕДЕРАЦИИ.....	301

Круть Леонид Сергеевич	
LEGAL TECH: ДРУГ ИЛИ ВРАГ ЮРИСТА?	307

Раздел VII

КИБЕРПРЕСТУПНОСТЬ, ТЕХНОЛОГИИ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Зуев Сергей Васильевич	
КРИЗИС СЛЕДСТВЕННОЙ ВЛАСТИ И ПЕРЕХОД НА ЦИФРОВОЕ ДОСУДЕБНОЕ ПРОИЗВОДСТВО ПО УГОЛОВНЫМ ДЕЛАМ	315

Степаненко Диана Аркадьевна, Рудых Алексей Александрович	
К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ МЕХАНИЗМА УДАЛЕННОЙ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ	319

Дерюгин Роман Александрович, Феклушина Анастасия Алексеевна	
О НЕКОТОРЫХ ВОПРОСАХ, СВЯЗАННЫХ С РАССЛЕДОВАНИЕМ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПРИМЕНЕНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ.....	328

Левченко Олег Викторович	
ПРОЦЕССУАЛЬНО-ПРАВОВАЯ ФОРМА ВЗАИМОДЕЙСТВИЯ ПРОКУРАТУРЫ И ОРГАНОВ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ ПРИ ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ.....	336

Бердникова Ольга Петровна, Блинова Ксения Николаевна	
НЕКОТОРЫЕ ОСОБЕННОСТИ ЛИЧНОСТИ МОШЕННИКА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ	345

Гаскаров Ильдус Фанавиевич, Ефимов Данил Сергеевич ОСОБЕННОСТИ ВЫЯВЛЕНИЯ И ДОКУМЕНТИРОВАНИЯ ФАКТОВ ВЗЯТОЧНИЧЕСТВА ПРИ ОСУЩЕСТВЛЕНИИ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.....	350
Долинин Владимир Николаевич, Шалудько Юлия Алексеевна ИСПОЛЬЗОВАНИЕ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ В РАССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ.....	361
Коломинов Вячеслав Валентинович СЛЕДСТВЕННАЯ СТРАТЕГИЯ В РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ.....	371
Никитина Елена Викторовна ЭЛЕКТРОННЫЕ СООБЩЕНИЯ КАК ОБЪЕКТ ПРОЦЕССУАЛЬНОГО ОСМОТРА	376
Табakov Александр Владимирович О ФОРМАХ ФИКСАЦИИ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ НА СОВРЕМЕННОМ ЭТАПЕ РАЗВИТИЯ КРИМИНАЛИСТИКИ	382
Архипова Екатерина Александровна ПРАВОВОЙ СТАТУС И ПРОЦЕДУРА ПРИЗНАНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В КАЧЕСТВЕ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ ПРОЦЕССЕ ИНОСТРАННЫХ ГОСУДАРСТВ	389
Иванов Эдуард Александрович О ТЕНДЕНЦИЯХ К ВЫСТРАИВАНИЮ СИСТЕМЫ ТЕХНОЛОГИЧЕСКОГО ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ЭКСТРЕМИЗМА.....	401
Медведев Виталий Александрович ПРИНЦИП РАБОТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ВЫЯВЛЕНИЯ НАРУШЕНИЙ ПРАВИЛ ДОРОЖНОГО ДВИЖЕНИЯ	406
Очеретько Елена Александровна, Попова Анна Алексеевна РОЛЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАССЛЕДОВАНИИ НЕРАСКРЫТЫХ ПРЕСТУПЛЕНИЙ ПРОШЛЫХ ЛЕТ	410
Иванов Владислав Юрьевич, Соколова Алёна Станиславовна ОСОБЕННОСТИ ДОПРОСА ЛИЦ, НАХОДЯЩИХСЯ НА САМОИЗОЛЯЦИИ В УСЛОВИЯХ ПАНДЕМИИ COVID-19.....	416

Караваева Анастасия Владимировна	
ЦИФРОВИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ	423
Лучинкин Федор Михайлович	
ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ОРД В ВИДЕ ЦИФРОВОЙ ИНФОРМАЦИИ В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ ...	429
Доронин Максим Вячеславович	
ПРОЦЕССУАЛЬНЫЕ УСЛОВИЯ И ПРОЦЕДУРА ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ	435
Ахметянова Виктория Эльдаровна	
ОСОБЕННОСТИ ИССЛЕДОВАНИЯ 3D-ОРУЖИЯ ПО БАЛЛИСТИЧЕСКОЙ ЭКСПЕРТИЗЕ.....	440
Глухов Никита Владимирович	
РОЛЬ ЦИФРОВИЗАЦИИ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ	443
Долгушина Полина Евгеньевна, Федосеева Виктория Сергеевна	
ИССЛЕДОВАНИЕ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ.....	449
Долгушина Полина Евгеньевна, Федосеева Виктория Сергеевна	
ПРЕДУПРЕЖДЕНИЕ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В РФ: ИНТЕГРАТИВНЫЙ И КОМПЛЕКСНЫЙ ПОДХОДЫ	456
Зиновенкова Алёна Андреевна, Сутягин Владимир Сергеевич	
ОТДЕЛЬНЫЕ АСПЕКТЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ	464
Зунгруев Аюка Витальевич, Медведев Виталий Александрович	
ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ	468
Капканникова Марина Алексеевна, Кочетова Елена Евгеньевна, Анисимова Алина Сергеевна	
КИБЕРПРЕСТУПНОСТЬ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ: МАСШТАБЫ, РИСКИ И МЕТОДЫ БОРЬБЫ	472
Кузбагаров Артур Муслимович	
ВИМ-МОДЕЛИРОВАНИЕ В ПРОИЗВОДСТВЕ СУДЕБНОЙ СТРОИТЕЛЬНО- ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ.....	478

Курбанова Фарахноз Хурshedовна	
ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ	484
Кускова Виктория Анатольевна, Цибирева Анна Сергеевна	
ПРИМЕНЕНИЕ МЕТОДА ТРЕХМЕРНОГО МОДЕЛИРОВАНИЯ В ЦЕЛЯХ УСТАНОВЛЕНИЯ ХРОНОЛОГИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ВЫПОЛНЕНИЯ ПЕРЕСЕКАЮЩИХСЯ ШТРИХОВ	489
Полтавский Богдан Сергеевич	
КАК ТЕХНОЛОГИИ ИЗМЕНЮТ ПОЛИЦЕЙСКУЮ ДЕЯТЕЛЬНОСТЬ.....	497
Темирова Алина Ильдаровна	
К ВОПРОСУ ОБ ОСОБЕННОСТЯХ ОРГАНИЗАЦИИ РАССЛЕДОВАНИЙ ПРЕСТУПЛЕНИЙ «ПО ГОРЯЧИМ СЛЕДАМ»	504
Шабунина Елизавета Алексеевна	
ЭКСПЕРТНЫЕ ОШИБКИ ПРИ ДНК-ИДЕНТИФИКАЦИИ: ВИДЫ, ПРИЧИНЫ, ЗНАЧЕНИЕ	509
Эмирбеков Фарид Язибекович	
ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В СЛЕДСТВЕННОМ КОМИТЕТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ	515

Раздел I

ОБЩИЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ И ЮРИДИЧЕСКОМ ОБРАЗОВАНИИ

Кодан Сергей Владимирович
Доктор юридических наук, профессор,
Заслуженный юрист Российской Федерации,
профессор кафедры теории государства и права,
Уральский государственный юридический университет
(г. Екатеринбург, Российская Федерация)
svk2005@yandex.ru

ЭЛЕКТРОННЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ В ИЗУЧЕНИИ ИСТОРИИ ПОЛИТИЧЕСКИХ И ПРАВОВЫХ УЧЕНИЙ*

Аннотация: В статье рассматриваются особенности использования электронных информационных ресурсов в исследовательских практиках изучения истории политических и правовых учений с позиций сочетания теоретических и прикладных подходов. Автором акцентируется внимание на конкретных сферах использования информационного подхода и современных информационных ресурсов в изучении источников по истории развития политико-правовой мысли. Обозначаются каналы взаимодействия познавательных средств и информационных ресурсов.

Ключевые слова: информатика, информационные ресурсы, юриспруденция, методология юридической науки, история политических и правовых учений, источники изучения политико-правовой мысли.

Для цитирования:

Кодан С. В. Электронные информационные ресурсы в изучении истории политических и правовых учений // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 13–22.

Использование информационных ресурсов в исследовательских практиках – не только характерная черта развития информационного общества, но и необходимый составной элемент современной методологии и технологии получения нового знания. Современный исследователь «погружен» в информационное

пространство и является субъектом информационных процессов, в рамках которых происходит обращение к носителям информации самого различного характера. Не является исключением в этом отношении и юридическая наука, для проведения исследований в которой активно используются различные информационные ресурсы и базы

* Публикация подготовлена в рамках реализации финансируемого РФФИ научного проекта № 20-011-00779 «Историография, источниковедение и методология истории политических и правовых учений: теоретические и прикладные проблемы исследовательских практик».

данных. При активном развитии юридической информатики как научной и прикладной дисциплины междисциплинарного характера, в её проблемных пространствах нерешёнными остаются вопросы конкретизации информационных технологий относительно их использования в исследовательских практиках в отдельных юридических науках.

В рамках представленного доклада и, соответственно, статьи позволю обратиться к проблематике информационного, методологического и технологического характера, связанной с возможностями применения современных информационных технологий в изучении конкретной юридической дисциплины – истории политических и правовых учений¹. При этом необходимо предварительно определиться с общим пониманием ряда вопросов, связанных с проблематикой использования информационных ресурсов в исследовании исторических процессов, и затем показать возможности использования современных исторических ресурсов в электронной форме их представления в исследовании развития политико-правовой мысли. Для этого выделим следующие вопросы.

¹ Данная статья продолжает проблематику, представленную автором на конференциях в 2019–2020 гг. См.: Кодан С. В. 1) Информационный подход в юридическом источниковедении // Технологии XXI века в юриспруденции: мат. Всеросс. научно-практ. конф. Екатеринбург, 2019. С. 70–75; 2) Информационные ресурсы в научно-исследовательских практиках // Технологии

1. Исторические информационные ресурсы в современных социально-гуманитарных науках выделяются в особую группу носителей информации и по их целевой направленности и рассматриваются как разновидность информационных ресурсов в целом и представляют собой носители информации, «относящиеся к предметной области исторической науки и образования» и обозначают их «принадлежность к исторической тематике»². Этот вид информационных ресурсов складывается вместе с историей человечества и представляет собой информационный процесс передачи сведений через исторические источники в качестве носителей информации о развитии различных сфер жизнедеятельности общества от поколения к поколению в диахронной проекции. Это подчёркивает И. Д. Ковальченко, обращая внимание на то, что «возникновение большинства исторических источников представляет собой информационный процесс, в котором фигурируют объект – отражаемая реальность, субъект – творец источника и информация – результат отражения объекта субъектом. Этот процесс, как и всякий информационный, всегда имеет прагматический аспект, т. е. творец

XXI века в юриспруденции: мат. Второй межд. научно-практ. конф. Екатеринбург, 2019. С. 14–22.

² См.: Корниенко С. И., Власова О. В., Гагарина Д. А. Исторические информационные ресурсы: понятие, описание, классификация // Информационные ресурсы России. 2012. № 1. С. 16–17.

источника всегда преследует определённую цель, выявляя сведения об объективной действительности»³.

Информационный обмен в контексте взаимодействия истории и современности исследуется на основе информационного подхода, который «состоит в изучении предельно разных объектов как информационных феноменов и процессов, как разновидностей и конкретных проявлений единой и весьма общей сущности информации». В указанном плане передача информации происходит посредством и форме исторических источников и при этом прежде всего должна учитываться общая схема передачи информации, которая включает: источник информации – канал связи с источником информации – приёмник информации. В исторической проекции указанная схема информационного взаимодействия усложняется и включает два этапа – «информационное взаимодействие на этапе создания источника» и «информационное взаимодействие на этапе прочтения источника историком». Соответственно общая схема передачи информации конкретизируется: «на первом этапе источником информации является сама эпоха, приёмником – автор будущего исторического источника. В качестве источника информации выступает любой объект прошлого,

сведения о котором фиксируются в источнике. На втором этапе источником информации служит уже исторический источник, а в качестве приёмника информации выступает прежде всего историк или любой человек, прочитавший источник и воспринявший какую-то часть информации, содержащейся в нём. Что же касается канала связи между объектом прошлого и историком, то в качестве такового можно рассматривать носитель информации, на котором зафиксированы сведения о прошлом, а также автора источника, зафиксировавшего данную информацию», – характеризуют процессы взаимодействия истории и современности в плане получения исторической информации Г. П. Можаяева и Н. А. Мишанкина⁴.

Исторические ресурсы в условиях информационного общества получают новые формы их представления в информационном пространстве и выступают уже как *электронные исторические информационные ресурсы*. При этом важно учитывать, что усложнение информационных потоков, формирование новых типов носителей информации и развитие информационных баз данных повлекло существенные изменения в организации, методологии и технологиях научных исследований и требует проработки теоретических и прикладных вопросов использования

³ Ковальченко И. Д. Методы исторического исследования. Изд. 2-е. М., 2003. С. 127–128.

⁴ См.: Можаяева Г. В. Историческая информация в контексте информологического подхода // Открытое и дистанционное образование. 2002. № 4. С.

170–174; Можаяева Г. П., Мишанкина Н. А. Информационный потенциал историографического источника в свете теории информации // Гуманитарная информатика. 2004. № 1. С. 114–125.

информационных ресурсов в исследовательских практиках. Особенно важным это становится и в контексте активного формирования общества знания как качественно нового состоянию социума, в основе которого «лежит возможность находить, производить, обрабатывать, преобразовывать, распространять и использовать информацию с целью получения и применения необходимых для человеческого развития знаний»⁵.

В группу исторических информационных ресурсов входят и источники по истории политических и правовых учений как историко-юридической науки, в предметную направленность которой входит «история возникновения и развития теоретических знаний о государстве, праве, политике и законодательстве, история политических и правовых теорий, история теорий права и государства»⁶. В отношении носителей информации по истории политико-правовой мысли применимы все указанные выше общие подходы к её исследованию в качестве исторических источников. При этом необходимо учитывать специфику источников информации в указанной сфере – ярко выраженную связь продуктов интеллектуальной деятельности с создавшими их субъектами и, соответственно, несущими личностные оценки и суждения относительно политических, государственных и правовых явлений и институтов, представленных в виде

доктринальных положений. Одновременно к указанной группе носителей информации относятся и историографический массив информации, показывающий развитие научных исследований в области истории и политических, и правовых учений и продляющий работы историков-юристов. Эти две группы исторических ресурсов их не исчерпывают весь массив исторической информации и включают другие исторические источники – проекты узаконений, материалы делопроизводства учебных, научных и цензурных учреждений, партийного, политического и идеологического надзора и контроля и др., которые образуют массив информационных ресурсов, необходимых для проведения исследований.

2. Исторические электронные информационные ресурсы и исследователь в условиях информационного общества тесно взаимосвязаны. И если первые создают информационное пространство для возможного использования электронных ресурсов в исследовательских практиках, то эффективность приложения этих возможностей для получения научного результата связана с личностными характеристиками учёного – опирается на его информационное мировоззрение, уровень информационной культуры и знания наличествующих баз электронных данных в сфере его познавательной деятельности. В связи с указанным обратим особое внимание

⁵ К обществам знания. Всемирный доклад ЮНЕСКО. Париж, 2005. С. 7.

⁶ Нерсисянц В. С. История политических и правовых учений. М., 2018. Т. 1. С. 11.

на то, что в современных условиях изменилось и положение учёного в пространстве научно-исследовательской деятельности – он в условиях интенсивно развивающегося информационного общества и его трансформации в общество знания получил уникальную возможность работы с продуктами интеллектуальной деятельности человека как материальным отражением и выражением в научной составляющей культурной памяти результатов познавательной деятельности.

Исторические электронные ресурсы позволяют исследователю получать на индивидуально-исследовательском уровне информацию, условно распределяемую по трём направлениям. Библиографическое направление получения информации состоит в получении общих сведений об источниках научной информации, необходимых для исследования. Здесь происходит электронная каталогизация документов и создание каталогов для электронного поиска взамен традиционных форм каталогов на бумажных носителях с их ручным поиском или просмотром в сканированном виде. Тем самым исследователь получает возможность оперативного поиска и просмотра библиографической информации о различного рода документах как носителях информации в электронной среде. Фактологическое направление получения информации обращено на обеспечение доступа непосредственно к источникам научной информации как носителям необходимых для исследования сведений и на этом

уровне представляется выход через аппаратные средства к цифровым версиям реальных бумажных документов (фотографии, сканы) -- изданных типографским способом, в машинописном виде или подготовленных в текстовых редакторах. Тем самым обеспечивается доступ для работы с документами в электронной визуальной форме как непосредственно в базе данных или получает возможность получения их копии в различных электронных форматах (DjVu, PDF и др.). Здесь исследователь получает возможность для работы с текстами в интерактивной среде на уровне зрительно-образного восприятия со всеми вытекающими из этого особенностями понимания и запоминания. Проблемно-ориентированное направление получения информации связано с обращением и общением исследователя с интеллектуально-поисковыми системами как инструментами поиска необходимой информации в различного рода базах данных и в сети Интернет. Тем самым создаётся и функционирует механизм наиболее тесного и плодотворного взаимодействия исследователя с фактографическими электронными базами данных, которые на основе библиографических сведений о реально существующих документах сосредотачивают их электронные версии, проблемно их ориентируют по предметно определённым областям на основе профессиональных семантических моделей представления и обработки знаний с использованием семантической

модели представления знаний, специальной лексики (языка) и позволяют пользователю получить доступ к различным фрагментам хранимой базы на основе широкой вариативности запросов к ней. Здесь исследователь получает возможность наиболее эффективно использовать информационные ресурсы в исследовательских практиках. В рамках указанных конкретных направлений познавательной деятельности учёным реализуется информационный подход к изучению источников социальной (в т. ч. и исторической) информации, выступающий как «способ приобретения, сохранения и использования информации, служащей достижению определённых целей в том смысле, что он должен привести к определённым результатам», — отмечает американский психолог Джером Брунер⁷.

3. Каналы использования электронных информационных ресурсов в изучении истории политических и правовых учений связаны с конкретными проблемными сферами/пространствами исследования развития политико-правовой мысли и источниками её познания. Современные электронные информационные ресурсы и технологии обеспечивают на принципиально новом уровне взаимодействие с носителями информации в изучении научной составляющей социальной памяти, научного наследия и преемственности

в научной деятельности. В рассматриваемых явлениях присутствует «специфическая надындивидуальная система информации, обеспечивающая накопление, хранение, передачу существенно важной, программирующей поведение индивидов информации от поколения к поколению (вертикальный обмен информацией), а также обмен информацией между людьми одного поколения (горизонтальный обмен информацией)»⁸.

Поэтому не случайно информационный подход в последние десятилетия выступает в качестве основного культурно-познавательного средства в изучении указанных явлений. При этом выделим три канала взаимодействия культурно-познавательных средств и информационных ресурсов. *Научная память и электронные информационные ресурсы* активно взаимодействуют в возможностях обращения к научной памяти как составляющей и вида социальной памяти, которая выступает как «совокупность социокультурных средств и институтов, осуществляющих отбор и преобразование актуальной социальной информации в информацию о прошлом (ретроспективную) с целью сохранения накопленного общественного опыта и передачи его

⁷ Брунер Дж. Психология познания. За пределами непосредственной информации / пер. с англ. М., 2008. С. 136.

⁸ Афанасьев В. Г. Социальная информация и управление обществом. М., 1975. С. 45–46.

от поколения к поколению»⁹. В этом информационном пространстве циркулируют продукты человеческой деятельности (включая и произведения мыслителей) и обеспечивается «связь между человеком и социумом через созданный одним и прочитанный "другими" интеллектуальный продукт предстаёт как эволюционно и глобально значимая: каждый созданный интеллектуальный продукт уже в момент своего создания пополняет совокупный ресурс человечества и может быть актуализирован теперь и всегда», — отмечает О. М. Медушевская¹⁰. Именно эти продукты человеческой деятельности выступают в качестве своеобразного «информационных посредников» между поколениями.

Современные информационные технологии в плане указанной выше «актуализации» интеллектуальных продуктов придают совершенно новое качество, связанное с возможностью оперативного и комплексного доступа к ранее территориально локализованным местам хранения носителей информации на уровне отдельных архивов, библиотек, музеев, галерей и др. «мест памяти», в которых, по замечанию французского историка Пьера Нора она «кристаллизуется и находит своё убежище»¹¹. Особенно значимым для развития информационного обмена в

сфере социальной памяти стало появление компьютерной техники, глобальных сетей передачи информации и информационных баз данных, которые обеспечили широчайшие возможности доступа к накопленной социальной памятью информации социально-гуманитарного характера. В современных условиях информационный обмен, связанный с социальной памятью, все больше носит не только надындивидуальный характер, но и выходит за рамки коллективной памяти отдельных групповых совокупностей людей и становится неотъемлемым элементом глобального информационного общества.

Научное наследие и электронные информационные ресурсы в своём взаимодействии обеспечивают обращение к социальному наследию, которое представляет «совокупность всей социальной информации, которой обладали уходящие из жизни поколения»¹². Его виды связаны и фрагментируются по сферам жизнедеятельности общества конкретным видам (историческое, культурное, научное юридическое, и др.). В указанном ряду особое значение в исследовательских практиках имеет обращение к научному наследию, которое содержит «опубликованные

⁹ Илизаров Б. С. Память социальная // Социологический словарь. М., 2008. С. 326–327.

¹⁰ Медушевская О. М. Теория и методология когнитивной истории // Собрание сочинений в 4 т. М., Берлин, 2017. С. 99. С. 65–418.

¹¹ См.: Нора П. Проблематика мест памяти // Франция-Память. СПб., 1999. С. 17.

¹² Илизаров Б. С. Роль ретроспективной социальной информации в формировании общественного сознания (В свете представлений о социальной памяти) // Вопросы философии. 1985. № 8. С. 60–69.

результаты научных исследований и экспериментов, библиографические и фактографические базы данных, сведения об учёных, их научной деятельности, публикациях, проектах и т. п., а также большое количество неопубликованных документов, таких как отчёты, письма, воспоминания, записки, фотоматериалы и т. п.»¹³ Соответственно электронные информационные ресурсы позволяют обеспечить обращение к научному наследию через соответствующие базы данных в различных формах и их конфигурациях. В полной мере это относится и политико-правовому наследию.

Научные электронные библиотеки в работе с научным наследием при помощи электронных информационных ресурсов являются главной формой обеспечения доступа к первоисточникам, книгам и текстам, которые находятся в крупнейших книгохранилищах страны. Среди них такие библиотечно-информационные ресурсы как Научная электронная библиотека eLIBRARY.RU, КиберЛенинка, Электронные библиотеки – Российской государственной библиотеки, Российской национальной библиотеки, Государственной публичной исторической библиотеки России и др. Активно развиваются и архивные базы данных, которые наряду развитием электронных каталогов, картотек, указателей, перечней и др. выставляют в электронной форме отдельные

архивные документы и их тематические подборки.

Преимущество в научных исследованиях и электронные информационные ресурсы взаимодействуют в плане расширения возможностей обращения к познавательному опыту и знаниям прошлого и позволяют обозреть значительные массивы различной научной информации, в т. ч. и сведений о развитии политико-правовой мысли. Этот канал связи, как указанные ранее, позволяет удовлетворить запросы исследователя на необходимость информационного обеспечения работы с носителями информации и получение достоверных эмпирических данных для научной работы. В указанных планах доступность, достоверность и надёжность информационных ресурсов при надлежащем использовании представляемых через их посредство носителей информации выступают одной из важнейших предпосылок обеспечения качества научных исследований, а информационные ресурсы позволяют обеспечить контроль за качеством исследовательского материала.

Итак, электронные информационные ресурсы в современных условиях становятся необходимой компонентой научно-исследовательских практик. Они позволяют расширить информационное пространство научного исследования и оптимизировать ход научного исследования. При этом исторические

методы и технологии, электронные коллекции. Тр. XV Всеросс. научн. конф. Ярославль, 2013. С. 91.

¹³ Барахнин В. Б., Федотов А. М., Федотова О. А. Электронная библиотека по научному наследию как фактографическая система // Электронные библиотеки: перспективные

электронные ресурсы выделились в носителей информации.
отдельную группу тематических

Список литературы

1. Афанасьев В. Г. Социальная информация и управление обществом. М., 1975. 408 с.
2. Барахнин В.Б. Электронная библиотека по научному наследию как фактографическая система / В. Б. Барахнин, А. М. Федотов, О. А. Федотова // Электронные библиотеки: перспективные методы и технологии, электронные коллекции. Тр. XV Всеросс. научн. конф. Ярославль, 2013. С. 91–97.
3. Брунер Дж. Психология познания. За пределами непосредственной информации / пер. с англ. М., 2008. 782 с.
4. Илизаров Б. С. Память социальная // Социологический словарь. М., 2008. С. 326–327.
5. Илизаров Б. С. Роль ретроспективной социальной информации в формировании общественного сознания (В свете представлений о социальной памяти) // Вопросы философии. 1985. № 8 С. 60–69.
6. К обществам знания. Всемирный доклад ЮНЕСКО. Париж, 2005. 231 с.
7. Ковальченко И. Д. Методы исторического исследования. Изд. 2-е. М., 2003. 486 с.
8. Кодан С. В. Информационные ресурсы в научно-исследовательских практиках // Технологии XXI века в юриспруденции: мат. Второй межд. научно-практ. конф. Екатеринбург, 2019. С. 14–22.
9. Кодан С. В. Информационный подход в юридическом источниковедении // Технологии XXI века в юриспруденции: мат. Всеросс. научно-практ. конф. Екатеринбург, 2019. С. 70–75.
10. Корниенко С. И. Исторические информационные ресурсы: понятие, описание, классификация / С. И. Корниенко, О. В. Власова, Д. А. Гагарина // Информационные ресурсы России. 2012. № 1. С. 16–19.
11. Медушевская О. М. Теория и методология когнитивной истории // Собрание сочинений в 4 т. М., Берлин, 2017. С. 65–418.
12. Можаяева Г. В. Историческая информация в контексте информологического подхода // Открытое и дистанционное образование. 2002. № 4. С. 170–174.
13. Можаяева Г. П. Информационный потенциал историографического источника в свете теории информации / Г. П. Можаяева, Н. А. Мишанкина // Гуманитарная информатика. 2004. № 1. С. 114–125.
14. Нерсесянц В. С. История политических и правовых учений. М., 2018. Т. 1. 482 с.
15. Нора П. Проблематика мест памяти // Франция-Память. СПб., 1999. С. 17–50.

Sergey V. Kodan

Doctor of Law, Professor, Honored Lawyer of the Russian Federation,
Professor of the Department of Theory of State and Law,
Ural State Law University
(Yekaterinburg, Russian Federation)
svk2005@yandex.ru

ELECTRONIC INFORMATION RESOURCES IN THE STUDY OF THE HISTORY OF POLITICAL AND LEGAL DOCTRINES

Abstract: The article discusses the features of the use of electronic information resources in research practices of studying the history of political and legal doctrines from the standpoint of a combination of theoretical and applied approaches. The author focuses on specific areas of using the information approach and modern information resources in the study of sources on the history of the development of political and legal thought. The channels of interaction between cognitive tools and information resources are indicated.

Keywords: informatics, information resources, jurisprudence, methodology of legal science, history of political and legal doctrines, sources of study of political and legal thought.

Бахтеев Дмитрий Валерьевич

Кандидат юридических наук, доцент, доцент кафедры криминалистики,

Уральский государственный юридический университет

(г. Екатеринбург, Российская Федерация)

ae@crimlib.info

Максимова Анастасия Валерьевна

Студент,

Уральский институт ГПС МЧС России

(г. Екатеринбург, Российская Федерация)

dekri08@mail.ru

ТЕХНОЛОГИЯ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ КАК ПОТЕНЦИАЛЬНЫЙ МЕТОД В ПРЕПОДАВАНИИ КРИМИНАЛИСТИКИ И ИЗУЧЕНИИ КРИМИНАЛИСТИЧЕСКИХ ОБЪЕКТОВ*

Аннотация: В статье проведён обзор технологии дополненной реальности (AR) с позиций социогуманитарного и криминалистического подходов, в том числе её актуальности, технологического минимума, в том числе методов реализации, а также областей применения, системы рисков и пределов использования. Кроме того, определена перспектива её внедрения в качестве метода преподавания криминалистики и изучения криминалистически значимых объектов.

Ключевые слова: дополненная реальность, аугментированная реальность, криминалистика, технология AR.

Для цитирования:

Бахтеев Д. В. Технология дополненной реальности как потенциальный метод в преподавании криминалистики и изучении криминалистических объектов / Д. В. Бахтеев, А. В. Максимова // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 23–30.

Всё большее развитие в современном мире приобретает дополненная реальность (технология augmented reality – AR), которая затрагивает различные сферы жизни: развлекательную, образовательную, промышленную и многие другие.

Однако к настоящему времени программная часть, методическое и нормативно-правовое обеспечение для реализации технологии дополненной реальности по данному направлению пока не достаточны.

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта 18-29-16001 «Комплексное исследование правовых, криминалистических и этических аспектов, связанных с разработкой и функционированием систем искусственного интеллекта».

Для реализации технологии AR в определённом направлении (в нашем случае – в качестве вспомогательного инструмента для изучения и преподавании криминалистики) необходимо прежде исследовать теоретические вопросы, связанные с данной технологией, находящиеся в том числе в междисциплинарном дискурсе, после чего создать прикладную информационную систему моделирования дополненной реальности (минимально – экспериментальный рабочий прототип базы данных, содержащий трёхмерные объекты, готовые для демонстрации).

Рассмотрим сущность технологии дополненной реальности с позиций социогуманитарного подхода. Дополненная реальность представляет технологию, функциональным назначением которой является добавление в визуальную воспринимаемую человеком картину реального мира (область видимого пространства) дополнительных виртуальных элементов, сгенерированные определённым алгоритмом на цифровом приборе, например, смартфоне или очках виртуальной реальности. Восприятие искусственных объектов и взаимодействие с ними происходит в режиме реального времени и эти объекты, отсутствуя в объективной реальности, появляются на дисплее устройства, гармонично встраиваясь в эту реальность. Последнее может проявляться в возможности

восприятия объекта под разными углами, с учётом эффектов светотени, эффектов массы, объема и прочих физических параметров.

История развития технологии AR началась с 1968 года, когда Иван Сазерленд и Боб Спрулл создали первый дисплей для ношения на голове, который был назван «Дамоклов меч».

Следующим этапом развития технологии AR принято считать разработку лаборатории искусственной реальности Videoplace Майроном Крюгером в 1974 году.

Спустя четыре года, в 1978-м, Стив Манн создал первое носимое AR-устройство EyeTap, в котором применялись камера и дисплей, дополняющий среду в режиме реального времени.

Несмотря на развитие данной технологии само понятие «дополненная реальность» появилось лишь в 1990 году в работе исследователей компании Boeing – Томаса Кауэлла и Дэвида Мизелла.

Дальнейшее развитие технологии дополненной реальности происходило стремительно, но только в рамках академических исследований и разработок или в очень специфических заводских условиях¹.

Всё изменилось лишь в 1999 году с выпуском ARToolKit, которая стала первой библиотекой с открытым исходным кодом для создания приложений дополненной реальности и включала библиотеку 3D-трекинга с использованием маркеров. Можно сказать, что с опубликованием данной

¹ Дополненная реальность – простое техническое введение // AR-студия «Третье декабря». URL:

https://veretennikov.info/dopolnennaya_realnost_prostoe_tekhnicheskoe_vvedenie (дата обращения: 26.04.2021).

библиотеки начался современный этап активного развития дополненной реальности.

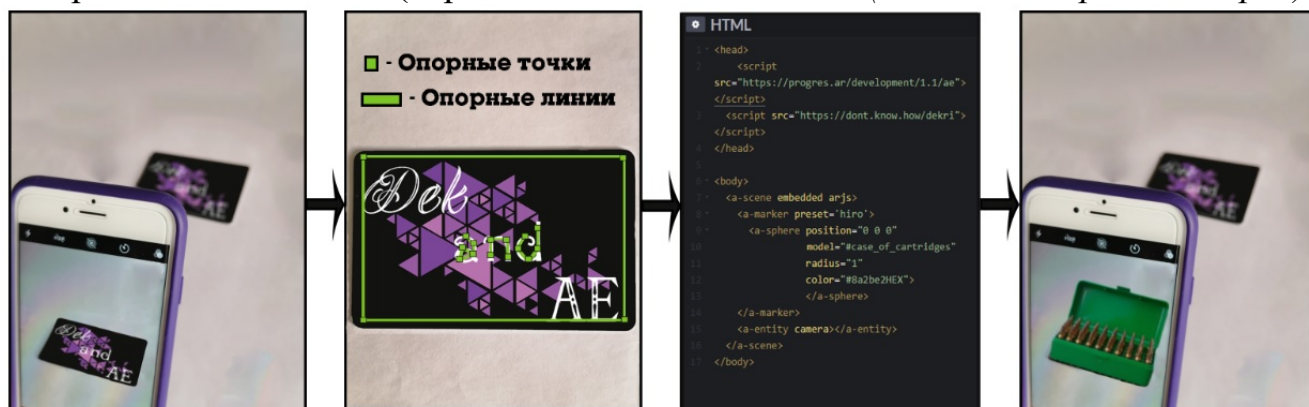
В настоящее время для воспроизведения дополненной реальности необходимы цифровые приборы, которые имеют следующие основные аппаратные компоненты: процессор, дисплей, датчики и устройства ввода. Самый доступный, но не менее удобный вариант – это современные смартфоны и планшеты, поскольку они оснащены геопозиционными (например, встроенные GPS и компас) и оптическими (цифровые камеры, выступающие в данном случае прозрачным видеодисплеем²) типами устройств, с помощью которых AR может получать информацию об окружающем мире.

Существуют три основных метода в структуре рассматриваемой технологии³:

1. Распознавание маркеров. Объектами в таком методе являются либо специально напечатанные изображения (черно-белый

квадратный маркер), либо любые объекты (например, визитка с изображением – приложение будет ориентироваться на некоторые опорные точки и линии на реальном объекте и использовать их в качестве маркера – см. Рис.1). Схема работы в этом случае начинается с наведения камеры устройства на объект с опорными точками, далее следует распознавание их с помощью программного кода, загрузка из базы приложения соответствующего маркерам графического объекта, помещение его в визуальную среду вместо изначального объекта. Соответственно в этом случае управление интеграцией оцифрованных объектов в объективную реальность, по большому счёту, осуществляется посредством размещения на местности (в помещении) предметов-маркеров.

Рис. 1. Распознавание опорных точек объекта (Источник: архив авторов)



² Distance Estimation with Mobile Augmented Reality in Action Space: Effects of Animated Cues / S. Chakraborty, J. K. Stefanucci, S. Creem-Regehr, B. Bodenheimer // IEEE Conference on Virtual Reality and 3D User

Interfaces Abstracts and Workshops (VRW). 2021. DOI: 10.1109/VRW52623.2021.00034.

³ Прокопов С. А., Соколовский Н. А. Основы и принципы работы технологии дополненной реальности // Решетневские чтения. 2018. Т. 2. С. 201–203.

2. Распознавание образов.

Объектами в таком методе являются реально существующие предметы, заранее загруженные в систему в качестве маркера. При наведении на такой объект произойдёт определённое действие, предусмотренное алгоритмом.

3. Безмаркерное наложение виртуальной «сетки» на окружающее пространство. Именно этот метод нами воспринимается как наиболее перспективный для решения ранее поставленных задач.

Указанные методы дополненной реальности свидетельствуют о том, что такая система может создаваться в виде приложения, что опять же подтверждает удобство и доступность использования.

Технология дополненной реальности уже используется в некоторых сферах жизни общества, и упрощает разрешение задач различного вида. К примеру, в медицине такие системы помогают в обучении проведении операций⁴; при осуществлении ремонтных работ и в производственных сферах – дают возможность производить живой просмотр 3D-схем и инструкций поверх реальных объектов⁵ и так далее.

Большое значение дополненная реальность играет и в сфере образования⁶. Это обуславливается рядом преимуществ по сравнению с традиционными средствами обучения, такими как визуализация сложных процессов, повышение мотивации и интереса к предмету, получение опыта и уменьшение количества значимых ошибок⁷, возможность обучения в удобном темпе и т. д.

При изучении криминалистики технология дополненной реальности позволит моделировать и реконструировать следовую информацию места происшествия либо материальной обстановки иного события в любых условиях. В настоящее время созданы системы моделирования обстановки места происшествия, но они носят стационарный характер, к примеру, в юридических вузах действуют криминалистические полигоны; в ведомственных вузах системы МЧС России созданы лаборатории для моделирования визуальной и акустической среды места пожара. Помимо этого, такие полигоны ограничены в количестве потенциальных моделируемых сценариев и зачастую не могут обеспечить должный уровень

⁴ Augmented Reality in Medical Practice: From Spine Surgery to Remote Assistance / F. Cofano, G. Di Perna, N. Mareng, [et al.] // *Frontiers in Surgery*. 2021. Vol. 8. Article: 657901. DOI:10.3389/fsurg.2021.657901.

⁵ Robot Devastation: Using DIY Low-Cost Platforms for Multiplayer Interaction in an Augmented Reality Game / D. Estevez, J. G. Victores, S. Morante, C. Balaguer // *EAI Endorsed Transactions on Collaborative Computing*. 2015. DOI: 10.4108/icst.intetain.2015.259753.

⁶ Rizov T., Rizova E. Augmented reality as a teaching tool in higher education // *International Journal of Cognitive Research in Science Engineering and Education*. 2015. Vol. 3 (1). P. 7–15. DOI:10.23947/2334-8496-2015-3-1-7-15.

⁷ Experimenting with electromagnetism using augmented reality: Impact on flow student experience and educational effectiveness / M. B. Ibáñez, Á. Di Serio, D. Villarán, C. Delgado Kloos // *Computers & Education*. 2014. Vol. 71. P. 1–13.

детализации, экспонируемые объекты показывают обстановку места происшествия «крупными мазками». Работа обучающихся в условиях полигона затруднена ограничением предельного количества одновременно занятых обучающимися, невозможностью использования в условиях заочных и дистанционных форм образования. Технология дополненной реальности в перспективе лишена указанных недостатков, что, в прочем, не исключает появления иных проблем.

Видится, что, помимо прочего, внедрение дополненной реальности в криминалистику затронет практическую деятельность, повлияет на научно-исследовательскую деятельность, в том числе молодых и начинающих учёных, а также позволит повышать квалификацию профессорско-преподавательскому составу.

Для практической деятельности технология может обеспечить дополнительную наглядность и информативность. Например, при рассмотрении дела суду помимо описания обстановки, фотографий и видеозаписей можно будет предложить графическое моделирование следовой картины и производную от неё систему интерпретации доказательственной информации. Таким образом возможно моделирование любых видимых материальных следов и объектов: следов крови, выстрела, поджога; орудий и средств совершения преступления и т. д.

В научно-исследовательской деятельности студенты выдвигают или выбирают гипотезы после сбора и анализа данных⁸, что в свою очередь приводит к дискуссиям и способствует научному интересу.

Таким образом, для целей криминалистики дополнительная реальность имеет следующий ряд преимуществ, как связанных с освоением и преподаванием учебного курса, так и имеющих потенциал быть взятыми на вооружение в практической деятельности:

- Возможность моделирования следовой информации по фабуле в условиях своего местонахождения, а не только на криминалистическом полигоне, что также облегчает процесс преподавания криминалистики в режиме дистанционного обучения.
- Доступность изучения и понимания криминалистики в различных условиях.
- Игрофикация процесса обучения.
- Увеличение наглядности и визуализации криминалистически значимых материальных объектов.
- Возможность изучения непосредственной следовой информации субъектами правоприменения (следователями, экспертами, прокурорами и судьями).

Для реализации данного проекта необходимо разработать программную часть, которая включает в себя не только один из методов реализации виртуальной реальности, но и базу данных с 3D-моделями,

⁸ Lund Nielsen B., Brandt H., Swensen H. Augmented Reality in science education—affordances for student learning // Nordic

Studies in Science Education. 2016. Vol. 12, № 2. P. 157–174. DOI:10.5617/nordina.2399.

которая может использоваться изолированно и создаваться в том числе на основе содержания криминалистических учётов. Сама сущность учёта представляет собой перекодирование информации, содержащейся в материальном объекте учёта – к примеру, следе подошвы обуви – в удобную для хранения форму. Аналогичная задача может разрешаться и при разработке системы дополненной реальности. Такой формой может быть запечатление следа двух- или трёхмерной съёмкой, либо преобразование объёмного или поверхностного объекта в совокупность количественных данных (методами линейного или углового измерения, расстановки и измерения реперных точек и т. д.).

Онтологические основы правового (в том числе криминалистического) изучения любой технологии предполагают учёт возможных рисков⁹. Применительно к технологии дополненной реальности условно их можно разделить на следующие категории: законодательные, организационно-управленческие и технические.

К **законодательным рискам** относится создание ограничительных нормативных требований к технологии дополненной реальности.

Организационно-управленческие риски:

- Неверная расстановка приоритетов, задач и этапов развития проекта.

- Неготовность материально-технической базы, к примеру, средств оцифровки материальных объектов.

- Некорректная оценка стоимости разработки, критериев подбора оцифровываемых объектов.

- Необходимость обучения технологии (при использовании интеллектуальных систем) в виде формирования датасетов для обучения.

- Контентные ошибки, например, в виде отсутствия отдельных узловых деталей на модели огнестрельного оружия.

Технические риски:

- Некорректное отображение объекта относительно окружения: например, неправильное отбрасывание тени или накладывание на другие объекты.

- Медленная работа приложения на более старых моделях смартфонов.

- Сбои системы, например, в виде произвольного закрытия приложения.

Не все риски можно избежать, однако, предусмотрев их, можно минимизировать возможную потерю базы данных, минимизировать возможные проблемы с быстродействием приложения при отображении объектов и т. д.

⁹ См.: Бахтеев Д. В. Современные технологии как предмет изучения и инструмент в юридических исследованиях и юридической деятельности // Технологии XXI века в юриспруденции: материалы Второй

международной научно-практической конференции (Екатеринбург, 22 мая 2020 года) Екатеринбург: Уральский государственный юридический университет. 2020. С. 23–29.

Пределы/недостатки использования дополненной реальности:

- Для правильного распознавания объекта и, соответственно, наложения на него виртуального объекта необходима хорошая освещённость. Другими словами, в малоосвещённых и тёмных помещениях устройство не сможет распознать среду.

- Для правильной идентификации объекта необходим его контраст с фоном (при использовании методов дополненной реальности, не рассматривающих специальные маркеры).

- Необходимость проработки базы для работы в иных помещениях

или перенос объектов с заранее определённым алгоритмом.

В целом, можно сделать вывод что технология AR является одним из перспективных направлений при изучении и преподавании криминалистики, которое имеет ряд преимуществ по сравнению с традиционными способами. Однако для реализации данного проекта требуется проработать множество различных аспектов, в том числе провести комплексное междисциплинарное изучение онтологических и технологических основ технологии дополненной реальности.

Список литературы

1. Бахтеев Д. В. Современные технологии как предмет изучения и инструмент в юридических исследованиях и юридической деятельности // Технологии XXI века в юриспруденции: материалы Второй международной научно-практической конференции (Екатеринбург, 22 мая 2020 года) Екатеринбург: Уральский государственный юридический университет. 2020. С. 23–29.

2. Дополненная реальность – простое техническое введение // AR-студия «Третье декабря». URL: https://veretennikov.info/dopolnennaya_realnost_prostoe_tekhnicheskoe_vvedeni.

3. Прокопов С. А. Основы и принципы работы технологии дополненной реальности / С. А. Прокопов, Н. А. Соколовский // Решетневские чтения. 2018. Т. 2. С. 201–203.

4. Augmented Reality in Medical Practice: From Spine Surgery to Remote Assistance / F. Cofano, G. Di Perna, N. Mareng, [et al.] // Frontiers in Surgery. 2021. Vol. 8. Article: 657901. DOI:10.3389/fsurg.2021.657901.

5. Distance Estimation with Mobile Augmented Reality in Action Space: Effects of Animated Cues / S. Chakraborty, J. K. Stefanucci, S. Creem-Regehr, B. Bodenheimer // IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW). 2021. DOI: 10.1109/VRW52623.2021.00034.

6. Experimenting with electromagnetism using augmented reality: Impact on flow student experience and educational effectiveness / M. B. Ibáñez, Á. Di Serio, D. Villarán, C. Delgado Kloos // Computers & Education. 2014. Vol. 71. P. 1–13.

7. Lund Nielsen B. Augmented Reality in science education—affordances for student learning / B. Lund Nielsen, H. Brandt, H. Swensen // Nordic Studies in Science Education. 2016. Vol. 12, № 2. P. 157–174. DOI:10.5617/nordina.2399.

8. Rizov T. Augmented reality as a teaching tool in higher education / T. Rizov, E. Rizova // International Journal of Cognitive Research in Science Engineering and Education. 2015. Vol. 3 (1). P. 7–15. DOI:10.23947/2334-8496-2015-3-1-7-15.

9. Robot Devastation: Using DIY Low-Cost Platforms for Multiplayer Interaction in an Augmented Reality Game / D. Estevez, J. G. Victores, S. Morante, C. Balaguer // EAI Endorsed Transactions on Collaborative Computing. 2015. DOI:10.4108/icst.intetain.2015.259753.

Dmitry V. Bakhteev

PhD (Law), Associate Professor of the Department of Criminalistics,
Ural State Law University
(Yekaterinburg, Russian Federation)
ae@crimlib.info

Anastasia V. Maksimova

Student,
Ural Institute of State Fire Service of EMERCOM of Russia
(Yekaterinburg, Russian Federation)
dekri08@mail.ru

**AUGMENTED REALITY TECHNOLOGY
AS A POTENTIAL METHOD IN TEACHING CRIMINALISTICS AND
EXAMING CRIMINALISTIC OBJECTS**

Abstract: The article provides an overview of augmented reality (AR) technology from the standpoint of socio-humanitarian and criminalistic approaches, including its relevance, technological minimum, implementation methods, as well as areas of application, system of risks and limits of use. In addition, the prospect of its implementation as a method of teaching forensic science and studying criminally significant objects has been determined.

Keywords: augmented reality, criminalistics, AR technology.

Каменев Александр Сергеевич
Адвокат Адвокатской палаты Челябинской области
(г. Челябинск, Российская Федерация)
kamenev_as@rambler.ru

ТРАНСФОРМАЦИЯ ФУНКЦИИ ЗАЩИТЫ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация: По мнению автора статьи, функция защиты как вид уголовно-процессуальной деятельности в настоящее время претерпевает значительные изменения, и это непосредственно связано с цифровизацией всей сферы уголовного судопроизводства. Цифровизацию можно рассматривать как условие, определяющее организацию и процессуальную сторону деятельности адвоката, а также других участников стороны защиты.

Ключевые слова: трансформация, цифровизация, адвокат, функция защиты, уголовное судопроизводство.

Для цитирования:

Каменев А. С. Трансформация функции защиты в уголовном судопроизводстве в условиях цифровизации // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 31–38.

Функция защиты как вид уголовно-процессуальной деятельности в настоящее время претерпевает значительные изменения (трансформацию), и связано это, прежде всего, с цифровизацией всей сферы уголовного судопроизводства. Цифровизацию можно рассматривать как условие, определяющее организацию и процессуальную сторону деятельности адвоката, а также других участников стороны защиты. В связи с этим представляет интерес: что и насколько существенно меняется в данном направлении, какие стороны этого явления затрагиваются.

Организация деятельности стороны защиты включает в себя: участие в проведении процессуальных действий и принятие решений в

дистанционном формате; ознакомление с процессуальными документами в электронном виде; направление жалоб, ходатайств, заявлений в органы государственной власти, занимающиеся производством по уголовным делам, посредством сети Интернет; сохранение конфиденциальности оказания юридической помощи с помощью мобильной связи. Процессуальная сторона функции защиты проявляет себя в собирании и представлении так называемых электронных доказательств, а также в инициировании их исследований; в оценке электронной информации, представленной стороной обвинения, включая методы идентификации и аутентификации.

Прежде всего, следует отметить процесс **автоматизации системы назначения адвоката** в порядке ст. 51 УПК РФ, который начался более 10 лет во многих адвокатских палатах и достаточно активно используется при распределении адвокатов в качестве защитников в уголовном судопроизводстве.

Необходимость перехода на цифровую систему назначения адвокатов, участвующих в качестве защитников в уголовном судопроизводстве по назначению органов дознания, предварительного следствия или суда, была продиктована в первую очередь борьбой с так называемыми «карманными адвокатами»¹.

Порядок назначения адвокатов в качестве защитников определил основные принципы назначения защитников по уголовным делам, такие как: независимость адвокатуры (исключение какого-либо влияния органов дознания, следствия, суда, иных органов и лиц на распределение требований о назначении защитника между конкретными адвокатами); равноправие адвокатов (право участвовать в делах по назначению вне зависимости от избранной формы адвокатского образования); территориальность (адвокат осуществляет защиту по назначению на территории субъекта, в котором сведения о нем внесены в реестр адвокатов); непрерывность (участие

адвоката с момента назначения до полного исполнения принятых обязательств, за исключением случаев, предусмотренных законодательством, соответствующим Порядком и Региональными правилами); централизация и информатизация (централизованное назначение адвокатов с использованием информационной системы автоматизированного распределения требований).

Вместе с тем, как отмечает Е. Н. Калачева, остаются не решенными еще многие проблемы. Во-первых, существует, так называемая, «двойная защита» («назначение адвоката-дублера»). Во-вторых, имеет место «притворное соглашение». В-третьих, наблюдаются попытки стороны обвинения с использованием автоматизированной системы получить наиболее «удобного» и «сговорчивого» адвоката².

Участие в процессуальных действиях и принятии решений по уголовным делам **в дистанционном формате** на сегодня не ограничивается осуществлением судебного разбирательства посредством видеоконференцсвязи. Ограничения в порядке передвижения в период пандемии создали определенные сложности для решения задач предварительного расследования в обычном режиме и подтолкнули правоприменителей к широкому использованию цифровых

¹ Под термином «карманный адвокат» понимают адвоката — защитника по назначению, появившегося в уголовном деле по инициативе следователя, действующего не в интересах подзащитного, «удобного» для стороны обвинения адвоката.

² Подробнее см.: Калачева Е. Н. Проблемы назначения адвоката-защитника в уголовном судопроизводстве и возможные пути решения: вызовы цифровизации // Вестник университета имени О. Е. Кутафина (МГЮА). 2020. № 11. С. 116.

технологий. Это коснулось, например, избрания меры пресечения в виде заключения под стражу. Осуществление заседания в режиме онлайн обеспечило возможность многим подозреваемым (обвиняемым) и их защитникам принять участие в этом независимо от места нахождения. Инициатором применения такой формы организации мог быть следователь или суд. Наличие возражений одной или обеих сторон по поводу рассмотрения уголовного дела или материала с использованием систем видеоконференцсвязи не могли быть препятствием для принятия судом такого решения. Определение порядка проведения судебного разбирательства в данном случае относится к исключительной компетенции суда, который исходил из необходимости обеспечения санитарно-эпидемиологической безопасности участников уголовного судопроизводства³.

А. М. Долгов справедливо отмечает, что производство предварительного расследования по уголовному делу, осуществляемое с использованием цифровых технологий, предполагает электронный документооборот по уголовному делу. При этом документооборот предполагает движение документов от отправителя (создателя) к получателю для

приобщения их к материалам уголовного дела или для дальнейшего направления к адресату. **Электронный документооборот** может осуществляться между различными участниками уголовного процесса, и здесь с одной стороны может быть адвокат или другой участник стороны защиты. К примеру, с помощью средств электронной связи, используя возможности сети Интернет, адвокат мог бы направлять жалобы и ходатайства соответствующим адресатам. Необходимо отметить, что возможность заявления ходатайств защитником принимает особое значение для результатов уголовного судопроизводства по каждому конкретному делу⁴.

В. А. Семенцов и Г. Г. Скребец пишут: «Если защитник обнаружил сведения, имеющие отношение к уголовному делу, но не получил их, он заявляет ходатайство суду, прокурору, следователю, дознавателю о проведении следственных действий, направленных на получение и закрепление в материалах уголовного дела указанных сведений. Поэтому в законе необходимо установить обязанность органа уголовного судопроизводства обеспечить участие защитника в проведении таких следственных действий»⁵. Это очень важное предложение, реализация

³ Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 3. Утвержден Президиумом Верховного Суда Российской Федерации 17 февраля 2021 года // Верховный суд: официальный сайт. URL:

<http://www.supcourt.ru/documents/all/29689/> (дата обращения: 10.05.2021).

⁴ Долгов А. М. Адвокат в электронном уголовном деле // Юридический вестник Кубанского государственного университета. 2019. № 1. С. 60.

⁵ Семенцов В. А., Скребец Г. Г. Формирование доказательств и участие

которого позволила бы в большей степени обеспечить состязательность и равноправие сторон.

Перспективность законодательной регламентации электронной формы документооборота между участниками стороны защиты и стороны обвинения (следователем, дознавателем, прокурором), безусловно, будет отвечать назначению уголовного судопроизводства и являться гарантией защищенности прав и законных интересов его участников.

Нельзя забывать о том, что сохранение адвокатской тайны – одна из главных обязанностей адвоката, прямо предусмотренных в ст. 8 Федерального закона от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»⁶.

Ю. С. Пилипенко считает, что адвокатская тайна «является специфическим признаком, отличительной особенностью адвокатской деятельности. Это то, без чего адвокатская деятельность трансформируется в сугубо консультационную, тот существенный признак, без которого и само явление теряет свою суть, свою содержательную сторону»⁷.

Решением Совета Федеральной палаты адвокатов РФ от 30.11.2009 (протокол № 3) утверждены Рекомендации по обеспечению

адвокатской тайны. Указанный документ является внутренним корпоративным актом адвокатуры, в нем содержатся необходимые разъяснения Совета Федеральной палаты адвокатов РФ по работе адвоката с информацией и необходимым мерах для **обеспечения сохранности и безопасности информации, полученной адвокатом** в ходе оказания юридической помощи.

В приложении № 2 к указанным Рекомендациям также приведен примерный перечень практических мер по защите информации, составляющей предмет адвокатской тайны. Данный перечень содержит несколько рекомендаций, относящихся собственно к хранению и передаче информации, составляющей охраняемую законом адвокатскую тайну, в электронном виде и к передаче ее через сеть Интернет. Одна из рекомендаций имеет непосредственное отношение к электронным коммуникациям: «Особое внимание уделить локальной сети, а также получению и отправке информации через Интернет, т. е. контролю за безопасностью электронной почты». В другой рекомендации предлагается «в телефонных разговорах с доверителем не касаться вопросов, в которые не должны быть посвящены посторонние»; в случае необходимости дополнительной

защитника в этом процессе // Уголовное право. 2007. № 4. С. 96.

⁶ Об адвокатской деятельности и адвокатуре в Российской Федерации: федеральный закон от 31.05.2002 № 63-ФЗ // СПС «КонсультантПлюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_36945/ (дата обращения: 10.05.2021).

⁷ Пилипенко Ю. С. Адвокатская тайна: Теория и практика реализации: автореф. дис. ... д-ра юрид. наук. М., 2009. С. 3.

защиты сведений, передаваемых доверителем при личном общении, использовать разные SIM-карты или телефонные аппараты; при обсуждении особо важных дел выключать сотовый телефон и вынимать из него батарею питания.

М. И. Коган справедливо отмечает, что цифровые технологии в последнее время существенно изменились, повлияв на возможности и способы их использования адвокатом, что, очевидно, приводит к необходимости доработки мер по обеспечению сохранения адвокатской тайны. Практически невозможно представить себе общение с доверителем без использования средств мобильной связи и электронной переписки. Несмотря на то, что наиболее важную информацию с доверителем многие адвокаты до сих пор предпочитают обсуждать лично, вероятность того, что такая конфиденциальна информация не будет упомянута, например, в ходе телефонного разговора, крайне низка⁸.

Далее, указанный автор предлагает меры, связанные с использованием адвокатом электронных устройств (мобильных телефонов, планшетов, ноутбуков), соблюдение которых позволит обезопасить конфиденциальную информацию в эпоху цифровизации. К таким мерам он относит:

1) обеспечение разумной защиты от потери мобильного устройства;

2) использование паролей на мобильных и иных электронных

устройствах, применяемых адвокатами, в том числе личных;

3) хранение полученной от доверителя информации на сервере адвокатского образования в зашифрованном виде; своевременное удаление такой информации с личных или недостаточно защищенных устройств;

4) обмен (получение и отправка) информации с доверителем посредством сети Интернет по общему правилу только в зашифрованном виде, особенно при использовании электронной почты.

Крайне важно иметь единые рекомендации по работе адвокатов с электронными устройствами, подготовленные с учетом практики адвокатской деятельности, а также при участии технических специалистов в сфере цифровых технологий. Актуальные общие рекомендации позволят адвокатскому сообществу иметь возможность применять единые актуальные критерии разумного поведения адвоката при обеспечении цифровой безопасности информации, полученной от доверителя.

Для обеспечения сохранности информации, которой оперирует защитник (адвокат) в электронной информационной среде, Е. В. Булгакова предлагает применять следующие средства: межсетевые экраны; антивирусную защиту; систему обнаружения вторжений; криптографическую защиту; защиту от утечек по техническим каналам; цифровые подписи; мониторинг и

⁸ Коган М. И. Обеспечение сохранения адвокатской тайны при использовании адвокатом современных технологий и

электронных девайсов // Вестник университета имени О. Е. Кутафина (МГЮА). 2020. № 11. С. 221.

управление ПБ серверов и АРМ. Все это, по мнению автора, можно реализовать посредством АРМ защитника (адвоката), с обеспечением, соблюдением режима доступа к ресурсам «Электронного правосудия»⁹.

Интерес представляет работа адвокатской палаты Воронежской области, где для общения с доверителями, находящимися в СИЗО, адвокатам был предложен специально выделенный видеоканал. Это опыт видеосвязи со следственным изолятором был признан достаточно успешным¹⁰ и может быть распространен на другие регионы.

Цифровые технологии института назначения адвоката динамично развиваются с учетом потребностей общества к формам и способам реализации конституционного права каждого на квалифицированную юридическую помощь, независимо от того, что оказывается она адвокатом по соглашению или по назначению.

Электронные доказательства, собранные и представленные стороной обвинения, подлежат тщательной проверке участниками

стороны защиты. Отсутствие четкой регламентации порядка копирования электронной информации и изъятия ее носителей дает возможность во всех случаях ставить под сомнение законность и допустимость полученных результатов. Статья 164.1 УПК РФ не в полной мере отвечает требованиям практики. Открытым остается и вопрос относительно того, что считать электронным носителем информации.

В литературе можно встретить такое понимание: электронный носитель информации – «это материальный предмет, содержащий процессуально значимую для уголовного дела электронную информацию, созданную вне производства по уголовному делу, восприятие которой невозможно без использования электронно-вычислительных средств»¹¹. Таким образом, под это понятие подпадает достаточно большой перечень оборудования, изъятие которого должно осуществляться в присутствии специалиста.

Немаловажным вопросом является идентификация¹² и аутентификация¹³. Необходимость в

⁹ Булгакова Е. В. Информационная безопасность защитника (адвоката). Организационно-правовой аспект // Правовая информатика. 2013. № 1. С. 42.

¹⁰ Жуков В. Защита на безопасной дистанции // Адвокатская газета. 2020. 25 ноя. URL: <https://www.advgazeta.ru/projects/ag-rakurs/zashchita-na-bezopasnoy-distantsii/> (дата обращения: 10.05.2021).

¹¹ Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / под ред. С. В. Зуева. М., 2020. С. 22.

¹² Под идентификацией понимается совокупность мероприятий по установлению сведений о лице и их проверке,

осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с уникальным обозначением (уникальными обозначениями) сведений о лице, необходимым для определения такового.

¹³ Аутентификация – это совокупность мероприятий по проверке лица на принадлежность ему идентификатора (идентификаторов) посредством сопоставления его (их) со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и установлению

этом может возникать при передаче данных, которые в дальнейшем используются в доказывании по уголовным делам. По сути, эти методы являются частью проверки на достоверность полученных сведений.

Идентифицировать можно по персональным данным, условным обозначениям имен, изображениям, прозвищам, номерам счетов, именам пользователей, удостоверениям личности, отпечаткам пальцев, образцам ДНК и большому разнообразию других способов. Следует признать, что методы идентификации не являются уникальными, многие из них могут быть подделаны, продублированы, смоделированы.

При аутентификации используются логины и пароли, пин-коды, ключевые слова и любая другая информация, которую человек может

запомнить и неоднократно воспроизвести. Эти данные используются для входа в учетные записи на персональных компьютерах. Особое значение в последнее время приобретает биометрическая аутентификация¹⁴.

В целом представляется, что трансформация призвана как на законодательном, так и на организационном уровне обеспечить максимальную эффективность реализации функции защиты в уголовном судопроизводстве. Многие проблемы могут быть решены с привлечением цифровых технологий и соответствующих программ, способных правовыми средствами отрегулировать баланс интересов участников уголовного процесса в стремлении к осуществлению правосудия.

Список литературы

1. Асаинова Л. С. Биометрическая аутентификация как альтернативный способ идентификации человека // Вестник науки и образования. 2020. № 9-3 (87). С. 63–67.
2. Булгакова Е. В. Информационная безопасность защитника (адвоката). Организационно-правовой аспект // Правовая информатика. 2013. № 1. С. 37–44.
3. Долгов А. М. Адвокат в электронном уголовном деле // Юридический вестник Кубанского государственного университета. 2019. № 1. С. 59–62.
4. Калачева Е. Н. Проблемы назначения адвоката-защитника в уголовном судопроизводстве и возможные пути решения: вызовы цифровизации // Вестник университета имени О. Е. Кутафина (МГЮА). 2020. № 11. С. 112–123.

правомерности владения лицом идентификатором (идентификаторами) посредством использования аутентифицирующего (аутентифицирующих) признака (признаков) в рамках процедуры аутентификации, в результате чего лицо считается установленным (ст. 2 Федерального закона

«Об информации, информационных технологиях и о защите информации» 29.12.2020 № 479-ФЗ).

¹⁴ Подробнее см.: Асаинова Л. С. Биометрическая аутентификация как альтернативный способ идентификации человека // Вестник науки и образования. 2020. № 9-3 (87). С. 63–67.

5. Коган М. И. Обеспечение сохранения адвокатской тайны при использовании адвокатом современных технологий и электронных девайсов // Вестник университета им. О. Е. Кутафина (МГЮА). 2020. № 11. С. 218–223.
6. Пилипенко Ю. С. Адвокатская тайна: Теория и практика реализации: автореф. дис. ... д-ра юрид. наук. М., 2009.
7. Семенцов В. А. Формирование доказательств и участие защитника в этом процессе / В. А. Семенцов, Г. Г. Скребец // Уголовное право. 2007. № 4. С. 93–97.
8. Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / под ред. С. В. Зуева. М., 2020. 193 с.

Alexander S. Kamenev
Attorney at Law of the Chelyabinsk Region
(Chelyabinsk, Russian Federation)
kamenev_as@rambler.ru

TRANSFORMATION OF THE PROTECTION FUNCTION IN CRIMINAL PROCEEDINGS IN THE CONDITIONS OF DIGITALIZATION

Abstract: According to the author of the article, the defense function as a type of criminal procedural activity is currently undergoing significant changes, and this is directly related to the digitalization of the entire sphere of criminal proceedings. Digitalization can be considered as a condition determining the organization and procedural side of defense lawyer's activity, as well as other participants of the defense.

Keywords: transformation, digitalization, lawyer, defense function, criminal proceedings.

Колесникова Наталья Сергеевна

Аспирант,

Московский государственный университет имени М. В. Ломоносова

(г. Москва, Российская Федерация)

n.s.kolesnikova@bk.ru

ПРОБЛЕМА ДОСТОВЕРНОСТИ ЗАКЛЮЧЕНИЯ СУДЕБНОГО ЭКСПЕРТА

Аннотация: Современная эпоха характеризуется сложностью информации. Изменения в информационных процессах затрагивают все сферы, включая правоприменительную деятельность. В результате этого в большинстве случаев следователю или суду невозможно установить обстоятельства, опираясь лишь на собственные знания, поэтому возникает потребность в использовании специальных знаний, обращении к сведущему лицу и получении такого важного доказательства как заключение эксперта. Вместе с тем, на сегодняшний день проблема достоверности заключения эксперта по-прежнему существует, поэтому требует решения. В статье анализируются примеры, основанные на судебной практике, дачи экспертом заведомо ложного заключения. Предлагаются пути решения данной проблемы.

Ключевые слова: судебная экспертиза, судебный эксперт, заключение эксперта, достоверность, профессиональная этика.

Для цитирования:

Колесникова Н. С. Проблема достоверности заключения судебного эксперта // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 39–42.

Сегодня проблема достоверности заключения эксперта по-прежнему существует, поэтому вызывает особое беспокойство. Недостоверными можно считать как неумышленно ошибочные, так и заведомо ложные заключения эксперта.

Как известно, за заведомо ложное заключение судебный эксперт несет уголовную ответственность, предусмотренную ст. 307 УК РФ, в производстве по делам об административных правонарушениях

– административную ответственность, предусмотренную ст. 17.9 КоАП РФ. Так, по данным статистики Судебного департамента Верховного суда РФ за первое полугодие 2020 года число осужденных за преступления, предусмотренные ст. 307 УК РФ, а именно: заведомо ложные показания, заключение эксперта, специалиста или неправильный перевод, составляло 207 человек. При этом необходимо учитывать, что статистика содержит суммарные показатели по всем составам преступлений,

предусмотренных ст. 307 УК РФ, а именно: заведомо ложные показания свидетеля, потерпевшего либо заключение или показание эксперта, показание специалиста, а равно заведомо неправильный перевод в суде либо в ходе досудебного производства.

Проанализируем приговоры различных судов, в соответствии с которыми лица признаны виновными в совершении преступления, предусмотренного ст. 307 УК РФ за дачу заведомо ложного заключения.

Эксперт К. при рассмотрении арбитражного спора дал заведомо ложное заключение строительно-технической экспертизы, на разрешение которой поставлены следующие вопросы:

1. Определить, по какому назначению могут быть использованы возведенные на земельном участке строения?

2. Определить, соответствуют ли возведенные на земельном участке строения градостроительным, строительным, противопожарным и иным обязательным нормам и правилам, выданным техническим условиям ресурсоснабжающих организаций?

В ходе проведения вышеуказанной судебной строительно-технической экспертизы и изготовления заключения эксперт К., имея умысел на дачу заведомо ложного заключения эксперта, осознанно и целенаправленно, достоверно зная о том, что срок действия предоставленных для проведения судебной строительно-технической экспертизы технических условий водоснабжения и

канализования объекта, составляющий 3 года на момент окончания исследования истек, договор подключения объекта капитального строительства с ресурсоснабжающей организацией не заключен, технологическое присоединение объекта к сетям водоснабжения и водоотведения не производилось, акт о подключении (технологическом присоединении) объекта не составлялся, к сетям водоснабжения и водоотведения в установленном законом порядке объект не подключен (имеется факт самовольного подключения к сетям водоснабжения), при ответе на поставленные судом вопросы, подготовил заведомо ложные не соответствующие фактическим обстоятельствам выводы, согласно которым все строительные конструкции, инженерное оборудование и сети исследуемых объектов находятся в работоспособном техническом состоянии, подключение сетей выполнено на основании технических условий, выданных соответствующими организациями, исследуемые объекты определены как соответствующие СНиП, возведенный на земельном участке объект может быть использован как многоквартирный жилой дом, который соответствует градостроительным, строительным и иным обязательным нормам и правилам, выданным техническим условиям ресурсоснабжающих организаций.

Таким образом суд пришел к выводу, что экспертом К. изготовлено представленное в Арбитражный суд в

ходе рассмотрения арбитражного дела заключение судебной строительно-технической экспертизы, содержащее заведомо ложные сведения о технических характеристиках объекта капитального строительства¹.

Эксперт А. при производстве дополнительной строительно-технической экспертизы, заведомо зная о неверном применении коэффициента, незаконно применил коэффициент $K=5,12$, который предназначен для формирования начальной (максимальной) цены торгов при подготовке конкурсной документации, общеэкономических расчетов в инвестиционной сфере для объектов капитального строительства, финансирование которых осуществляется с привлечением средств федерального бюджета, который не предназначен для взаиморасчетов за выполненные работы, то есть, применив указанный коэффициент без взаиморасчета между Г. и Р. и завысив в локальной смете стоимость объемов выполненных ремонтно-строительных работ здания техстанции, дал заведомо ложное заключение о том, что общая стоимость ремонтно-строительных работ и материалов с учетом НДС, проведенных по реконструкции здания, в уровне цен на момент производства исследования составляет 10 038 753 рубля, хотя реальный объем и их стоимость составляет 2 810 168 рублей, тем

самым завысил их выполнение на 7 228 585 рублей, что повлекло вынесение Ленинским районным судом решения о взыскании с Г. стоимости объемов выполненных ремонтно-строительных работ по объекту здания техстанции и возможного причинения ей ущерба на указанную сумму.

Таким образом, А. совершил преступление, предусмотренное ч. 1 ст. 307 УК РФ, то есть дал заведомо ложное заключение эксперта в суде².

При этом результаты проведенного опроса показали, что 83,3 % следователей, 50 % судей, учитывая собственный практический опыт, считают, что количество осужденных экспертов по ст. 307 УК РФ не соответствует реально существующему количеству заведомо ложных заключений эксперта, поэтому данное преступление является высоколатентным.

Это объясняется тем, что имеются сложности в установлении умысла на дачу заведомо ложного заключения, поскольку при допросе эксперт в свою защиту может сказать о том, что допустил ошибку. Для установления умысла эксперта на заведомо ложное заключение целесообразно провести оперативно-розыскные мероприятия, например, прослушивание телефонных переговоров, контроль сообщений, а также проанализировать заключения этого же эксперта по другим делам, в которых он сделал противоположные

¹ Приговор Ленинского районного суда г. Ростова-на-Дону от 22.05.2019 по делу № 1-216/2019 // СудАкт. URL: <https://sudact.ru/> (дата обращения: 05.05.2021).

² Приговор Советского районного суда г. Махачкалы (Республика Дагестан) от 10.11.2015 по делу № 1-744/2015 // СудАкт. URL: <https://sudact.ru/> (дата обращения: 05.05.2021).

или отличающиеся выводы. Кроме того, необходимо проанализировать заключения других экспертов по схожим судебным экспертизам, а также обратиться к специалисту для рецензирования заключения эксперта.

Эксперт в теории процессуального права понимается как лицо, содействующее правосудию. Содействовать правосудию можно только будучи принципиально честным, независимым, квалифицированным, компетентным в соответствующей области знаний, искусства, техники или ремесла.

Исходя из этого, судебным экспертом должно быть такое лицо, которое действительно осознает свое предназначение в содействии правосудию. На наш взгляд, формированию такого образа мышления эксперта может помочь профессиональная этика, положения которой необходимо совершенствовать и разрабатывать для целей судебно-экспертной деятельности. Это позволит снизить существующие проблемы, в том числе проблему недостоверных заключений.

Natalia S. Kolesnikova

Postgraduate student,
Lomonosov Moscow State University
(Moscow, Russian Federation)
n.s.kolesnikova@bk.ru

THE PROBLEM OF THE RELIABILITY OF THE FORENSIC EXPERT'S OPINION

Abstract: The modernity is characterized by the complexity of information. Changes in information processes affect all areas, including law enforcement. As a result, in most cases it is impossible for an investigator or a court to establish the circumstances relying only on their own knowledge, therefore, there is a need to use special knowledge, contact a competent person and obtain such important evidence as an expert opinion. At the same time, today the problem of the reliability of the expert's opinion still exists, therefore it requires a solution. The article analyzes examples, based on judicial practice, of knowingly giving false expert opinion. The ways of solving this problem are suggested.

Keywords: forensic examination, forensic scientist, expert opinion, reliability, professional ethics.

Шашкова Ирина Алексеевна

Магистрант,

Самарский национальный исследовательский университет

имени академика С. П. Королёва

(г. Самара, Российская Федерация)

irina.shashkova.2013@mail.ru

Научный руководитель – В. Э. Волков, кандидат юридических наук, доцент
кафедры государственного и административного права

ОСНОВНЫЕ НАПРАВЛЕНИЯ РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЩЕСТВЕННЫХ ОТНОШЕНИЙ

Аннотация: В целях защиты интересов граждан государство принимает меры по локализации данных о гражданах путем законодательного регулирования российского сегмента Интернета. Однако, как показывает практика, в том числе и судебная, имеющиеся средства защиты персональных данных являются недостаточными в условиях использования новых технологий. Вместе с тем практика применения законодательства о персональных данных выявляет ряд проблем, которые требуют своего решения.

Ключевые слова: персональные данные, обезличивание, массив данных, база данных, идентификация субъектов.

Для цитирования:

Шашкова И. А. Основные направления регулирования защиты персональных данных в условиях цифровой трансформации общественных отношений // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 43–49.

В рамках создания благоприятных условий и новых возможностей для использования и обращения информации (данных) в интересах потребителей, бизнеса, общества и государства в целом, необходимым видится разработка дополнительных правовых и иных механизмов защиты прав и свобод субъектов персональных данных, активно участвующих в общественных отношениях.

В сфере регулирования данных и государство, и бизнес уделяют гораздо больше внимания вопросам защиты персональных данных. Указанные тенденции можно объяснить как относительной удовлетворенностью действующим регулированием права изготовителя базы данных, так и еще недостаточной потребностью в использовании этого права. Нередко компании, обладающие фактическим контролем

над большими массивами данных, защищают их техническими средствами и используют их самостоятельно. В других случаях компании передают или обрабатывают массивы данных на основании гражданско-правовых договоров, но при этом не заявляют исключительного права на базу данных и не используют договорные конструкции части четвертой ГК РФ. В то же время если обратиться к судебной практике, то дело ООО «ВКонтакте» против ООО «ДАБЛ», хотя и является пока единичным, может служить хорошей иллюстрацией тех преимуществ, которыми наделяет обладателей Больших пользовательских данных право изготовителя базы данных¹.

Важным средством защиты персональных данных является также обезличивание данных о конкретном лице.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого,

выгодоприобретателем или поручителем по которому является субъект персональных данных. Обработываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей (ч. 7 ст. 5 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ).

Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, утверждены Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

В соответствии с приказом одним из собственных признаков обезличенных данных выступает анонимность (невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации).

В Европейском союзе достаточно много внимания уделяется выработке методологий обезличивания персональных данных. Наиболее подробным документом в этой

¹ Суд разрешил резиденту «Сколково» сбор данных пользователей «ВКонтакте» // РБК. URL:

https://www.rbc.ru/technology_and_media/12/02/2021/60267e8f9a79474fbd968df3 (дата обращения: 20.03.2021).

области является Позиция рабочей группы по статье 29 «О методологиях обезличивания данных»². Данный документ делит все методы обезличивания на две большие группы, основанные на введении случайных данных в исходный массив информации (randomisation) и обобщении значений некоторых параметров исходного массива информации (generalisation). Помимо традиционных методологий, отраженных, в том числе в Приказе Роскомнадзора № 996 (перемешивание, обобщение данных, введение идентификаторов), Позиция рабочей группы вводит ряд инновационных методологий, например differential privacy (дифференциальная приватность), представляющая собой особый способ доступа к информации на основе метода «запрос-ответ» и имеющая в своей основе математические алгоритмы добавления «шума» в исходные данные, к которым делается запрос на получение информации³.

С мая 2018 г. в Европе действуют новые правила обработки персональных данных, установленные Общим регламентом по защите данных (Регламент ЕС 2016/679 от 27.04.2016, GDPR – General Data Protection Regulation). Названный Регламент имеет прямое действие в 28 странах ЕС. С его принятием утратила силу Директива о защите персональных данных 95/46/ЕС от

24.10.1995. Важной особенностью GDPR является экстерриториальный принцип действия новых европейских правил обработки персональных данных, а также усиление ответственности за нарушение правил обработки персональных данных: штрафы достигают 20 млн. евро (около 1,5 млрд руб.).

Отсюда очевидна необходимость изменения российского законодательства в части значительного усиления ответственности за нарушения законодательства о персональных данных.

В настоящее время ведется активная проработка вопроса обезличенных данных. Первым шагом на закрепление на законодательном уровне стала разработка в 2019 году законопроекта о внесении изменений в Федеральный закон «О персональных данных». Данный проект предусматривал дополнение новым понятийным аппаратом, в том числе такими понятиями, как «обезличенные персональные данные», «обезличенные данные». Также в связи с этим предусматривалась дача согласия на обезличивание персональных данных, в том числе в целях их последующей передачи третьим лицам. Несмотря на то, что данный законопроект не был внесен в Государственную Думу Российской Федерации, данные

² Opinion 05/2014 on Anonymisation Technics. Article 29 Data Protection Working Party (10 April 2014). // European Commission: official site. URL: <https://ec.europa.eu/justice/article-29/documentation/opinion->

[recommendation/files/2014/wp216_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf). P. 20 (accessed: 20.03.2021).

³ Dwork C. Differential privacy // Proceedings of the 33rd international conference on Automata, Languages and Programming. 2006. Vol. Part II. P. 1.

положения имеют место быть рассмотренными и в настоящее время.

Усиление внимания к проблеме было вызвано и Посланием Президента Российской Федерации Федеральному Собранию Российской Федерации от 15 января 2020 года № Пр-113 в части защиты прав и свобод человека и гражданина при обработке его персональных данных, и обеспечения регулирования оборота больших объемов данных⁴, после которого началась активная законодательная работа по внесению изменений в Федеральный закон «О персональных данных».

В марте 2021 года Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Министерство) вместе с профильными министерствами разрабатывает поправки в законопроект №992331-7 «О внесении изменений в ФЗ «О персональных данных», одобренный Государственной Думой в первом чтении 16 февраля 2021 года, предусматривающие, в том числе дачу разрешения субъекта не только на использование сведений о нем, но и на их обезличивание⁵. Отметим, что данное положение однозначно коррелируется с вышеописанными ранее невнесенными в Государственную Думу поправками.

Обмен обезличенными данными, по задумке Министерства, будет

возможен только между государственными структурами и отечественными IT-компаниями, причем органы государственной власти будут получать их исключительно для осуществления функций государства. Например, это может понадобиться для анализа различных вариантов развития транспортной инфраструктуры. По словам ведомства «бизнес и сейчас сдает в государственные органы статистическую отчетность, но эта отчетность не позволяет принимать решения».

Законопроект регламентирует политику обработки обезличенных данных. Например, теперь оператор не сможет использовать какую-либо дополнительную информацию, которая помогает определить принадлежность персональных данных конкретному субъекту. Также будет запрещено в дополнение к обезличенным данным передавать третьим лицам информацию, которая позволит идентифицировать конкретного человека. Под запретом окажется «деобезличивание данных», за исключением тех случаев, когда необходимо защитить жизнь или здоровье человека. Использовать обезличенные данные без согласия пользователя можно будет только в исследовательских и статистических целях.

⁴ Перечень поручений по реализации Послания Президента Федеральному Собранию (утв. Президентом РФ 24.01.2020 № Пр-113) // Официальный сайт Президента РФ. URL: <http://www.kremlin.ru/acts/assignments/orders/62673> (дата обращения: 29.03.2021).

⁵ Законопроект № 992331-7 О внесении изменений в Федеральный закон «О персональных данных» (в части уточнения порядка обработки персональных данных) // Система обеспечения законодательной деятельности. URL: <https://sozd.duma.gov.ru/bill/992331-7> (дата обращения: 29.03.2021).

Следующим этапом можно отметить модернизация системы аналитики больших объемов данных о жителях столицы. Подведомственное департаменту информационных технологий (далее – ДИТ) Москвы государственное казенное учреждение (ГКУ) «Информационный город» до конца августа 2022 года хочет создать подробную и персонализированную базу данных о каждом жителе Москвы, которая будет интегрирована с другими информационными системами для взаимного обогащения данными. В их числе Единая система идентификации и аутентификации и автоматизированная информационная система многофункциональных центров.

Как следует из технического задания к закупке, планируется создать интерактивную «витрину» с обезличенной информацией о жителях столицы и систему обмена этими данными с «внешними потребителями». Предполагается доработать «информационную систему управления данными в распределенной вычислительной среде» (ИС УДРВС). Сейчас она интегрирована с большинством информационных систем города, включая Единую мобильную платформу и Единую геоинформационную систему.

Среди анализируемых данных – основные события, связанные с гражданином, информация об их объектах недвижимости и транспорте и счетах за коммунальные услуги. ДИТ хочет сделать систему визуализации собранных данных. Предполагается, что пользователь через интерфейс сможет видеть

данные об имуществе горожан, тратах на ЖКХ и другую статистику. «Внешними потребителями» обновленной информационной системы могут стать также компании, которые оказывают услуги горожанам.

При этом профили пользователей государственных услуг в Москве будут содержать большой объем персональных данных. Среди них кроме номеров паспортов, СНИЛС, ИНН, полиса ОМС и других документов, которые уже и так содержатся в тех или иных ГИС, будут, например, данные о фактическом месте жительства, родственниках, транспорте (VIN, ПТС, СТС), месте работы, номер карты «Тройка» и даже данные о питомцах. Новый сервис, по мнению экспертов, сведет в одном месте все уже собранные данные, ускорив предоставление государственных услуг, но одновременно и повысит опасность утечки информации.

Также эксперты считают, что город идет по пути максимальной централизации хранения данных и управления ими, что должно снизить объемы неточностей и неактуальных данных. Сбор информации поможет, например, давать субсидии: по сумме доходов домовладения можно выяснить потребность и автоматически их назначить.

Но многие эксперты видят и риски. Заместитель председателя комиссии по правовому обеспечению цифровой экономики московского отделения Ассоциации юристов России Александр Савельев считает, что власти Москвы целенаправленно собирают большие массивы данных о

гражданах, чтобы создать систему, подобную китайской. По его словам, граждан могут вынуждать давать обширные согласия на обработку данных в момент обращения в московские структуры и учреждения, а также передавать их с помощью «манипуляций с доступностью» льгот и государственных услуг.

Кроме того, любая централизованная система может рассматриваться как потенциальный источник утечки. Защита мегахранилищ обычно намного сложнее и дороже, чем взлом. «Централизация данных всегда ведет к повышению рисков утечек и неавторизованного доступа. В этом плане куда безопаснее выглядит

модель, реализованная в Скандинавских странах, которая позволяет не хранить данные в одном месте, а безопасно обмениваться ими заинтересованным сторонам».

В итоге хотелось бы подчеркнуть следующее: несмотря на принятие новых законов, а также принятие государственными органами подзаконных актов, среди которых особое значение имеют акты Роскомнадзора, правовое регулирование отношений по использованию и защите персональных данных все же требует законодательного «переосмысления», в том числе с учетом опыта зарубежных стран.

Список литературы

1. Романова А. Ю. К вопросу о правовом режиме Больших данных // Конституционное и муниципальное право. 2019. № 8.
2. Савельев А. И. На пути к концепции регулирования данных в условиях цифровой экономики // Закон. 2019. № 4.
3. Савельев А. И. Направления регулирования Больших данных и защита неприкосновенности частной жизни в новых экономических реалиях // Закон. 2018. № 5.
4. Солдатова В. И. Защита персональных данных в условиях применения цифровых технологий // Lex russica. 2020. № 2.

Irina A. Shashkova

Graduate student,
Samara National Research University
named after Academician S. P. Korolev
(Samara, Russian Federation)
irina.shashkova.2013@mail.ru

Scientific supervisor – V. E. Volkov, PhD (Law), Associate Professor of the
Department of State and Administrative Law

**MAIN DIRECTIONS OF REGULATION OF PERSONAL DATA
PROTECTION IN THE CONDITIONS OF DIGITAL TRANSFORMATION OF
PUBLIC RELATIONS**

Abstract: In order to protect the interests of citizens, our state takes measures to localize data about citizens by legislative regulation of the Russian segment of the Internet. However, as practice shows, including judicial practice, the available means of protecting personal data are insufficient in the context of the use of new technologies. At the same time, the practice of applying the legislation on personal data reveals a number of problems that need to be addressed.

Keywords: personal data, depersonalization, data array, database, identification of subjects.

Адалина Алина Александровна

Студент,

Национальный исследовательский Нижегородский государственный университет
имени Н. И. Лобачевского

(г. Нижний Новгород, Российская Федерация)

adalinaalina798@gmail.com

Научный руководитель – Ю. В. Жильцова, кандидат экономических наук, доцент
кафедры судебной экспертизы

СОВРЕМЕННОЕ ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ФИНАНСОВО-ЭКОНОМИЧЕСКОЙ ЭКСПЕРТИЗЫ

Аннотация: В статье анализируется и раскрывается суть информационных технологий в практике финансово-экономической экспертизы. Исследуется актуальность использования современного информационного обеспечения. Раскрываются основные проблемы недостаточности информационного обеспечения экспертов, а также выдвигаются предложения по их решению.

Ключевые слова: финансово-экономическая экспертиза, информационные технологии, информационное обеспечение, судебная экспертиза.

Для цитирования:

Адалина А. А. Современное информационное обеспечение финансово-экономической экспертизы // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 50–56.

Реалии сегодняшнего уровня развития экономической системы говорят о ведущем значении информации, своевременное использование которой оказывает прямое воздействие на результативность деятельности компании. Оперативно обрабатывать, накапливать и передавать многочисленные потоки данных помогают информационные технологии, которые, в общем виде, предполагают использование

компьютеров, программного обеспечения, коммуникаций, сетей для удовлетворения информационных потребностей¹.

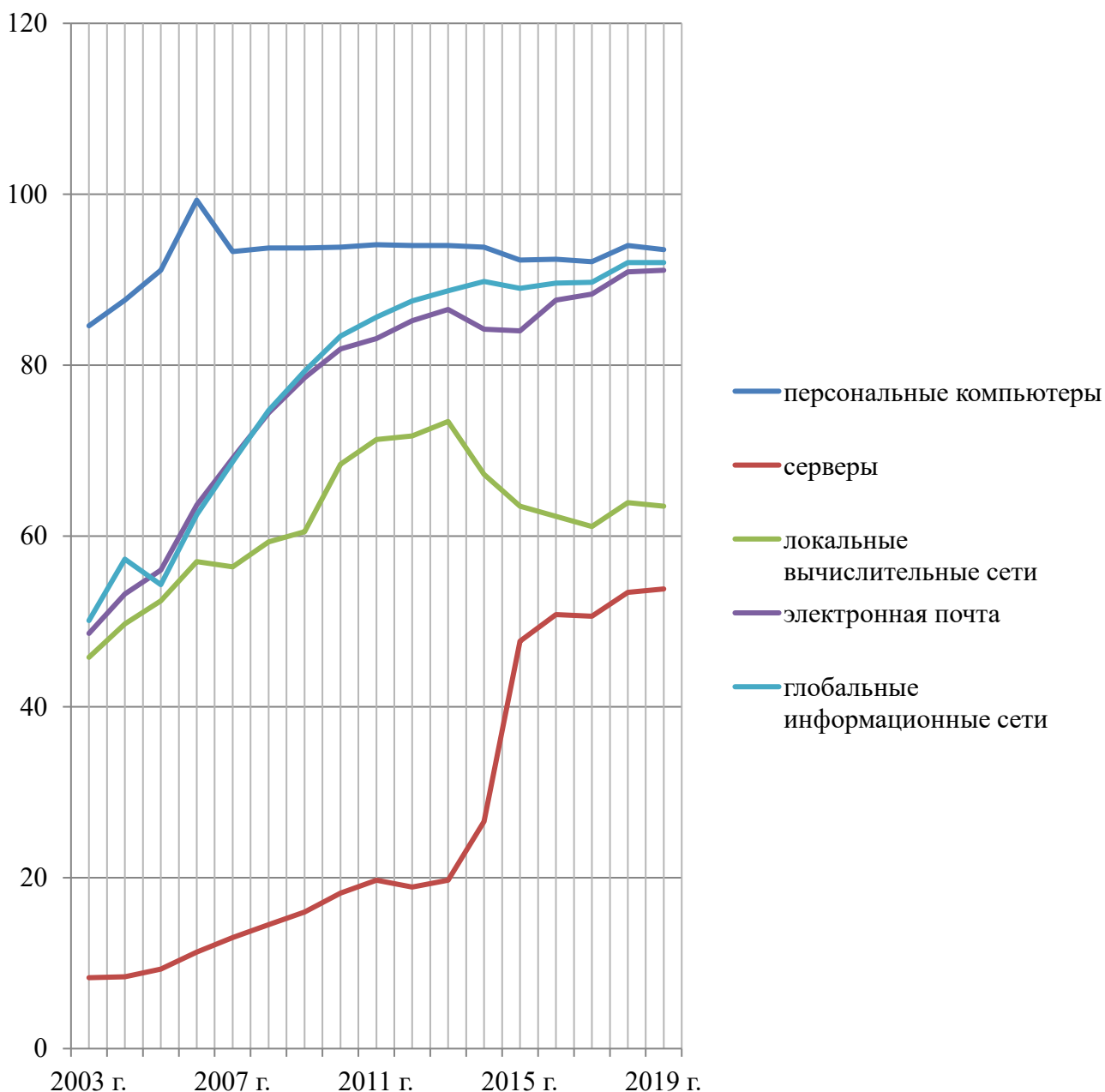
Увеличение числа компаний, применяющих в своей деятельности информационные технологии, подтверждают, в том числе, статистические сведения. Так, по данным Федеральной службы государственной статистики, вырос удельный вес организаций, использовавших информационные и

¹ Володченко В. С., Ланцова Д. С., Миронова Т. А. Понятие и классификация

информационных технологий // Достижения науки и образования. 2020. № 12 (66). С. 41.

коммуникационные технологии, в период с 2003 г. по 2019 г.² Быстрыми темпами осуществляется внедрение серверов, электронной почты и глобальной информационной сети (см. Рис.1).

Рис. 1. Удельный вес организаций, использовавших информационные и коммуникационные технологии в период с 2003 г. по 2019 г., в % от общего числа.



² Наука, инновации и информационное общество. Информационное общество // Федеральная служба государственной

статистики: официальный сайт. URL: <https://rosstat.gov.ru/folder/14478> (дата обращения: 22.03.2021).

Информационные технологии активно используются не только в деятельности организаций, но и в деятельности правоохранительных органов, в том числе, при производстве экономических экспертиз. Информационное обеспечение экспертной деятельности позволяет эксперту эффективнее накапливать, обрабатывать и передавать информацию, а также избежать совершения экспертных ошибок.

Нынешнее развитие экономической и хозяйственной деятельности часто требует экспертных проверок и оценок. Так, при расследовании дел о преднамеренном и фиктивном банкротстве нередко возникает необходимость в проведении судебной финансово-экономической экспертизы. Судебная финансово-экономическая экспертиза – это комплекс судебных экономических исследований, целью которых является определение финансового положения организации, установление финансовых проблем, анализ финансово-экономических показателей компании (в том числе процесса формирования этих показателей).

В расследованиях экономических преступлений главным источником информации о составе преступления, способе совершения, исполнителе и прочих обстоятельствах, свидетельствующих о преступной деятельности или создании условий для такой

деятельности, являются финансовые (бухгалтерские) документы, учитывающие факты экономической деятельности хозяйствующего субъекта. Финансовые (бухгалтерские) документы имеют юридическую силу, а также устанавливают ответственность исполнителей за совершаемые ими финансовые и коммерческие операции. Для эксперта важно профессионально использовать информационные технологии для проведения финансово-экономических проверок. Компании часто используют программы компьютерного учета, такие как «1С: Бухгалтерия», «БЭСТ 2», «БЭСТ 3», «Парус», «Инфин-Бухг» и ряд других.

Информационные технологии, разрабатываемые в настоящее время для судебной экономической экспертизы, направлены на выявление признаков определенных противоправных действий. Как показывает современная практика, преступления в экономической сфере в настоящее время совершаются таким образом, что действия преступников закономерно оставляют следы в бухгалтерской (финансовой) отчетности, а также оказывают воздействие на финансовые показатели организации. По этой причине в экономических исследованиях необходимо использовать качественный логико-информативный анализ документальных данных, основанный на различных методах и приемах³:

³ Ваниева А. А., Грудаева Ю. В. Информационные технологии и информационное обеспечение судебно-

экономической экспертизы // Экономика, управление, финансы: материалы III

- разработка экономических и информационных моделей и сравнение с эталонными моделями;
- диагностический анализ неточностей исследуемых систем;
- сравнение показателей (бухгалтерских записей);
- группировка;
- подведение показателей к сопоставимости;
- детализация показателей (записей);
- подстановка;
- сравнение балансовых отчетов;
- процентные соотношения;
- корреляционный, факультетский (альтернативный) и регрессивный анализ;
- информационно-нормативный анализ;
- табличные конструкции;
- блок-схемы и др.

Принимая во внимание специфику проведения финансово-экономической экспертизы, нужно признать, что информационные технологии занимают важное место при проведении экспертизы, так как начальный этап подготовки этого рода экспертизы заключается в анализе финансовой информации, и последующем расчете коэффициентов, характеризующих различные аспекты финансового положения организации. Так, например, для определения типа устойчивости организации могут

использоваться следующие коэффициенты:

- коэффициент обеспеченности собственными оборотными средствами;
- коэффициент обеспеченности собственными оборотными и приравненными к ним средствами;
- коэффициент обеспеченности запасов всеми источниками;
- коэффициент автономии и т. д.

Расчет перечисленных коэффициентов предполагает выполнение экспертом простейших арифметических операций на основе информации, представленной в бухгалтерской (финансовой) отчетности. Нахождение значений данных коэффициентов относится к прямым расчетным задачам, так как предполагает получение результата по формуле, исходя из заданных показателей⁴. Несмотря на то, что данные расчеты не представляют сложности для эксперта, экспертом могут совершаться ошибки, например, из-за утраты возможности качественного проведения анализа в результате исследования значительного объема бухгалтерских (финансовых) документов.

В связи с этим, представляется возможным использовать информационные технологии, например, программные комплексы, пакеты прикладных программ, для проведения необходимых расчетов.

Междунар. науч. конф. (г. Пермь, февраль 2014 г.). Пермь: Меркурий, 2014. С. 89–93.

⁴ Одинцов Б. Е., Романов А. Н., Догучаева С. М. Современные информационные

технологии в управлении экономической деятельностью. Москва: ИНФРА-М, 2020. С. 180–182.

Стоит отметить, что оценка полученных при расчете результатов экспертом осуществляется путем их сравнения с нормативными показателями, установленными для каждого коэффициента. Таким образом, при помощи информационных технологий может производиться не только расчет коэффициентов, но и выявление несоответствий между полученными результатами и установленными нормативными показателями⁵.

Однако, в данном случае, возникает другая проблема – нормативные показатели могут различаться, например, для разных отраслей экономики, что значительно осложняет проведение анализа полученных результатов, как самим экспертом, так и программными комплексами. В таких обстоятельствах целесообразно дать возможность экспертам-экономистам самостоятельно варьировать значения нормативных показателей в рамках использования информационных технологий.

Кроме того, серьезной проблемой при проведении финансово-экономической экспертизы является отсутствие единой информационной базы для экспертов-экономистов, отсутствие комплексной межведомственной координации научно-методической работы в этой области, а также реализация отдельных научно-технических рекомендаций в области экспертных технологий разными ведомствами. Это приводит к ряду

негативных последствий, которые можно наблюдать на макроуровне: неэффективное распределение финансовых, человеческих, материальных и технических ресурсов; дублирование экономических исследований; спад эффективности результатов судебно-экономической экспертизы.

Использование информационных технологий, компьютеризация и создание единой информационной базы данных – все это значительно облегчает работу экономического эксперта. Однако из практики экспертной финансово-экономической деятельности видно, что рекомендации и предложения по внедрению информационных технологий в деятельность финансово-экономической экспертизы реализованы не полностью. По данным МВД Российской Федерации, в настоящее время 100 % экспертов используют компьютер для расследования экономических преступлений. На практике, при этом, только 10 % используют автоматизированные методы исследования в своей работе.

Использование информационных технологий при проведении финансово-экономической экспертизы позволяет выявлять и оценивать факты искажения экономической информации, выявлять и количественно оценивать негативные экономические явления и ситуации, связанные с ними, а также определять уровень зависимости от этих ситуаций

⁵ Ищенко А. Н. Автоматизация процесса производства судебно-экономических экспертиз как способ устранения типичных

ошибок в экспертной деятельности // Статистика и экономика. 2015. № 1. С. 76.

и явлений финансовых результатов хозяйствующего субъекта. Поэтому при использовании информационных технологий для выполнения финансово-экономической экспертизы необходимо учитывать нормы правового обеспечения экспертной деятельности и действующее законодательство.

Признание важности роли информационных технологий и их организационной составляющей в создании эффективных методов проведения финансово-

экономических экспертиз подводит к выводу о том, что для фиксирования их в механизме экспертной деятельности необходимо им дать правовую оценку, а также разработать и закрепить методику их применения. Исключительно в этом случае организационные методы использования информационных технологий для изучения финансовых документов и бухгалтерских записей при проведении экономических экспертиз станут обязательными.

Список литературы

1. Ваниева А. А. Информационные технологии и информационное обеспечение судебно-экономической экспертизы / А. А. Ваниева, Ю. В. Грудяева // Экономика, управление, финансы: материалы III Междунар. науч. конф. (г. Пермь, февраль 2014 г.). Пермь: Меркурий, 2014. С. 89–93.
2. Володченко В. С. Понятие и классификация информационных технологий / В. С. Володченко, Д. С. Ланцова, Т. А. Миронова // Достижения науки и образования. 2020. № 12 (66). С. 41–43.
3. Ищенко А. Н. Автоматизация процесса производства судебно-экономических экспертиз как способ устранения типичных ошибок в экспертной деятельности // Статистика и экономика. 2015. № 1. С. 75–77.
4. Наука, инновации и информационное общество. Информационное общество // Федеральная служба государственной статистики: официальный сайт. URL: <https://rosstat.gov.ru/folder/14478>.
5. Одинцов Б. Е. Современные информационные технологии в управлении экономической деятельностью / Б. Е. Одинцов, А. Н. Романов, С. М. Догучаева. Москва: ИНФРА-М, 2020. 373 с.

Alina A. Adalina

Student,

National Research Lobachevsky State University of Nizhny Novgorod

(Nizhny Novgorod, Russian Federation)

adalinaalina798@gmail.com

Scientific supervisor – Yu. V. Zhiltsova, PhD (Economics), Associate Professor of the Department of Forensic Science

MODERN INFORMATION SUPPORT OF FINANCIAL AND ECONOMIC EXPERTISE

Abstract: The article analyzes and reveals the essence of information technology in the practice of financial and economic expertise. The relevance of the use of modern information support is examined. The main problems of insufficient information support of experts are revealed, as well as proposals for their solution are put forward.

Keywords: financial and economic expertise, information technology, information support, forensic expertise.

УДК 349

Кириленко Анна Сергеевна

Студент,

Крымский юридический институт (филиал)

Университета прокуратуры РФ

(г. Симферополь, Республика Крым, Российская Федерация)

AnnInCannes@yahoo.com

Сахипова Сауле Ассаматовна

Студент,

Крымский юридический институт (филиал)

Университета прокуратуры РФ

(г. Симферополь, Республика Крым, Российская Федерация)

sahipova.s@mail.ru

Научный руководитель – Г. А. Гундериц, кандидат технических наук,
доцент, юрист 2 класса

ПРАВОВОЕ ОБЕСЕПЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: В данной статье анализируется законодательство в сфере обеспечения информационной безопасности Российской Федерации. Рассмотрено развитие правовой базы в данной сфере. В соответствии с Доктриной информационной безопасности Российской Федерации в статье рассмотрены основные составляющие интересов в информационной сфере.

Ключевые слова: информационная безопасность, правовое обеспечение информационной безопасности, национальная безопасность, Стратегия национальной безопасности, Доктрина информационной безопасности Российской Федерации.

Для цитирования:

Кириленко А. С. Правовое обеспечение информационной безопасности в Российской Федерации / А. С. Кириленко, С. А. Сахипова // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 57–62.

Значительное усиление влияния информационной сферы на жизнь человека, жизнь общества и государства является одной из характерных тенденций общественного развития второй

половины XX – начала XXI веков. Это связано, с одной стороны, с качественно новыми достижениями научно-технической революции в области компьютерных технологий и телекоммуникаций, которые

значительно повышают эффективность информационной деятельности, а с другой стороны, с признанием прав человека и свободы в информационной сфере основными ценностями современного общества.

В содержании интересов общества все более значимое место занимает «информационная» составляющая, отражающая заинтересованность в защите прав и свобод человека в сфере информационной деятельности, в совершенствовании национальной информационной инфраструктуры и в гарантировании устойчивого функционирования данной инфраструктуры в развитии «информационной» экономики как одного из ключевых сегментов национальной экономики¹.

Правовое обеспечение информационной безопасности — относительно самостоятельная область информационного права, которая состоит из правовых режимов, принципов и норм, содержащихся в законодательстве Российской Федерации и источниках международного права. Данное направление регулирует общественные отношения в области обеспечения безопасности, в первую очередь, информации и информационной инфраструктуры, которые используются людьми, обществом и государством для

преследования законных интересов, а также для осуществления законных прав и обязанностей².

Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации.

Между тем, влияние информационных технологий и ресурсов оказывает значительное влияние на состояние экономической сферы: в зависимости от полноты и достоверности необходимых данных, а также своевременности их получения, защищенности сведений, являющихся коммерческой тайной, увеличивается зависимость от информационной сферы.

Обороноспособность и безопасность государства напрямую зависят от качества получаемой информации, уровня информационных технологий, безопасности систем обработки информации и связи, используемых разведкой, контрразведки, радиоэлектронной борьбы, командования и контроля войсками и оружием³.

Под информационной безопасностью Российской Федерации понимается состояние защищенности личности, общества и государства от внутренних и внешних

¹ Стрельцов А. А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы: учебное пособие. Москва, 2018. С. 4–6.

² Полякова Т. А., Стрельцов А. А. Организационное и правовое обеспечение информационной безопасности: учебник и

практикум для СПО. М.: Юрайт, 2020. С. 24–26.

³ Алексеева Е. В. Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере // Ленинградский юридический журнал. 2016. № 4. С. 98–99.

информационных угроз, гарантирующее реализацию конституционных прав и свобод человека и гражданина, качество и стандарт достойной жизни граждан, суверенитет, территориальную целостность и устойчивое социально-экономическое развитие Российской Федерации, оборону и безопасность государства.

Как самостоятельная составляющая национальной безопасности, информационная безопасность одновременно оказывает непосредственное влияние на защиту интересов Российской Федерации в экономической, международной, общественной, федеральной, оборонной и других сферах жизни общества.

Конституция Российской Федерации (далее – Конституция РФ), как основной закон, содержащий в себе основополагающие права и обязанности граждан Российской Федерации, содержит в себе правовые основы информационной безопасности.

В период с 1995 г. по 2006 г. основным законодательным актом, который регулирует общественные отношения в информационной сфере в Российской Федерации (далее – РФ), являлся Федеральный закон РФ «Об информации, информатизации и защите информации», правовую основу которого составляла Конституция РФ 1993 г. Данный закон в качестве основных положений содержал в себе вопросы формирования и использования

информационных ресурсов, создания и использования информационных технологий, защиты информации и др. (п. 1 ст. 1). Одним из приоритетных направлений государственной политики являлось обеспечение национальной безопасности в сфере информатизации (п. 2 ст. 3).

На смену указанному выше закону пришел новый акт – Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», которым существенно дополнялась правовая база обеспечения информационной безопасности.

31 декабря 2015 г. Указом Президента Российской Федерации В. В. Путиным была утверждена и введена в действие обновленная Стратегия национальной безопасности Российской Федерации. В основу Стратегии были заложены положения ранее действовавшей Стратегии 2009 г.

Исходя из положений пункта 113 Стратегии, наибольшее внимание уделяется созданию и обеспечению информационной безопасности с учетом национальных стратегических приоритетов. При интерпретации положений Стратегии становится очевидным, что информационная безопасность является методологически важным элементом национальной безопасности. Сама стратегия полностью ориентирована на вопросы национальной безопасности в различных сферах⁴.

⁴ Яхьяева М. И. Информационная безопасность как составная часть национальной безопасности Российской

Федерации // Государственная служба и кадры. 2020. № 2. С. 42–44.

Ключевым концептуальным документом в области информационной безопасности является Доктрина информационной безопасности, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 года. Этот документ отражает позицию официальной власти в отношении таких понятий, как функции, задачи и принципы обеспечения безопасности информации Российской Федерации. Настоящая Доктрина вместе с федеральными законами, иными нормативными правовыми актами Российской Федерации и федеральных органов исполнительной власти, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации составляет правовую основу в области информационной безопасности.

В частности, как видно из текста документа, Доктрина является актом стратегического планирования в области обеспечения национальной безопасности Российской Федерации, развивающим положения Стратегии национальной безопасности Российской Федерации, утвержденной Указом. Президента Российской Федерации от 31 декабря 2015 г. № 6839 и других документов о стратегическом планировании в этой сфере.

Кроме того, она служит основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности Российской Федерации; разработки мероприятий по совершенствованию системы защиты информации.

Доктрина акцентирует внимание на следующих основных составляющих национальных интересов Российской Федерации в информационной сфере:

а) гарантия и защита конституционных прав человека и гражданских прав и свобод в части, которая касается получения и использования информации, конфиденциальности при использовании информационных технологий, обеспечения информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также использование информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

б) обеспечение стабильного и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой телекоммуникационной сети Российской Федерации, в мирное время, при неминуемой угрозе агрессии и в военное время;

в) развитие в Российской Федерации электронной промышленности и информационных технологий, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и использованию средств обеспечения информационной безопасности,

оказанию услуг в области обеспечения информационной безопасности;

г) предоставление российскому и международному сообществу достоверной информации о государственной политике Российской Федерации и ее официальной позиции в отношении социально значимых событий в стране и мире, использование информационных технологий для обеспечения национальной безопасности Российской Федерации в области культуры;

д) содействие в создании международной системы информационной безопасности, направленной на противодействие угрозам использования информационных технологий для нарушения стратегической

стабильности, укрепление равноценного стратегического партнерства в области информационной безопасности, а также защита суверенитета Российской Федерации в информационном пространстве⁵.

Таким образом, по своей направленности и структуре новая Доктрина информационной безопасности РФ является логическим продолжением Стратегии национальной безопасности РФ. Указанное обстоятельство должно в перспективе позволить выстраивать всю совокупность документов в сфере информационной безопасности с учетом соответствующих стратегических национальных приоритетов.

Список литературы

1. Алексеева Е. В. Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере // Ленинградский юридический журнал. 2016. 4. С. 98–99.
2. Полякова Т. А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов. М.: Юрайт, 2020. С.24–26.
3. Стрельцов А. А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы: учебное пособие. Москва, 2018. С. 4–6.
4. Яхьяева М. И. Информационная безопасность как составная часть национальной безопасности Российской Федерации // Государственная служба и кадры. 2020. № 2. С. 42–44.

⁵ Доктрина информационной безопасности Российской Федерации: указ Президента Российской Федерации от 05.12.2016 г. № 646 // Офиц. интернет-портал правовой

информации. URL: <http://publication.pravo.gov.ru/Document/View/0001201612060002> (дата обращения: 14.05.2021).

Anna S. Kirilenko

Student,

Crimean Law Institute (branch) of the University of the Russian prosecutor's office
(Simferopol, Republic of Crimea, Russian Federation)

AnnInCannes@yahoo.com

Saule A. Sakhipova

Student,

Crimean Law Institute (branch) of the University of the Russian prosecutor's office
(Simferopol, Republic of Crimea, Russian Federation)

sahipova.s@mail.ru

Scientific supervisor – G. A. Gunderich, PhD (Technical Sciences),
Associate Professor, lawyer of the 2nd class

LEGAL SUPPORT OF INFORMATION SECURITY IN THE RUSSIAN FEDERATION

Abstract: This article analyzes the legislation in the field of information security of the Russian Federation. The development of the legal framework in this area is considered. In accordance with the Information Security Doctrine of the Russian Federation, the article considers the main components of interests in the information sphere.

Keywords: information security, legal support of information security, national security, National Security Strategy, Information Security Doctrine of the Russian Federation.

Чепурнов Вадим Александрович

Студент,

Саратовская государственная юридическая академия

(г. Саратов, Российская Федерация)

v.chep9717@yandex.ru

Научный руководитель – А. С. Анисимова, кандидат юридических наук, старший преподаватель кафедры информационного права и цифровых технологий

РЕГУЛЯТОРНЫЕ «ПЕСОЧНИЦЫ» НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ: ПРАВОВАЯ РЕГЛАМЕНТАЦИЯ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ В ОТЕЧЕСТВЕННОМ ПРАВЕ

Аннотация: Данная работа посвящена рассмотрению регуляторных песочниц, которые до настоящего момента остаются без детального правового регламентирования. Анализируется их содержание, назначение и перспективы внедрения в России. Делается акцент на проблемы, которые затрудняют рассмотрение регуляторных песочниц в рамках российского права.

Ключевые слова: регуляторные песочницы, экспериментальные правовые режимы, цифровые инновации, цифровой рынок, юридическое лицо.

Для цитирования:

Чепурнов В. А. Регуляторные «песочницы» на территории Российской Федерации: правовая регламентация и перспективы применения в отечественном праве // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 63–67.

28 января 2021 года на территории России вступил в силу Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»¹. Данный нормативный акт давно ожидался в сфере отечественного правового поля. Он позволил субъектам экспериментального правового режима создавать, так называемые,

регуляторные «песочницы», в пределах которых они смогут временно отменять действующие законодательные ограничения, в случае если это понадобится для нормального функционирования режима. Такой подход зачастую используется в международной практике. Так, широкое распространение он получил в следующих странах мира:

¹ Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации: федеральный закон от 31 июля

2020 г. № 258-ФЗ // Российская газета. 2020. 6 авг.

Великобритания, Канада, Сингапур, Австралия, где по нынешний день он является неотъемлемой частью развития цифровых технологий, конкуренции, обеспечения развития науки и социальной, финансовой сферы и других отраслей.

Так как экспериментальный режим, согласно п. 4 ч. 2 ст. 1 указанного Федерального закона, сферой своего действия устанавливает область цифровых и информационных инноваций, следовательно, возникает вопрос о перспективах его применения и целях, устанавливаемых законодателем, а также устанавливает потребность в проведении сравнительного анализа на основе мировых моделей представляемого режима.

Регуляторные «песочницы» — это особые правовые режимы, которые позволяют юридическим лицам, занимающимся разработкой новых продуктов и услуг, проводить в ограниченной среде эксперименты по их внедрению, избегая риск нарушения законодательства².

Основными целями Российской регуляторной песочницы, согласно статье 3 Федерального закона «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», являются: формирование новых видов и форм экономической деятельности, способов осуществления экономической деятельности; повышение эффективности

государственного или муниципального управления; совершенствование общего регулирования по результатам реализации экспериментального правового режима; развитие конкуренции; привлечение инвестиций в развитие предпринимательской деятельности в сфере цифровых инноваций в Российской Федерации и другие.

Так, организация, желающая участвовать в экспериментальном режиме, вносит инициативное предложение в уполномоченный орган (законодатель уточнения о конкретном органе не делает) с проектом программы режима, после чего уполномоченный орган проверяет соответствие инициатора требованиям и условиям осуществления эксперимента, затем предложение вносится в Правительство РФ, где принимается окончательное решение об одобрении или отказе в участии инициатора.

Статья 6 того же закона оговаривает условия возможности субъекта принятия участия в эксперименте, таким образом, у субъекта должна существовать технологическая возможность применения цифровых инноваций, а также не должно быть у инициатора (индивидуального предпринимателя, лица, осуществляющего функции единоличного исполнительного органа, либо члена коллегиального исполнительного органа или совета

² Куклина Е. А. «Регулятивные песочницы» как эффективный механизм реализации цифровой повестки // Большая Евразия: Развитие, безопасность, сотрудничество. 2019. С. 265–268. Режим доступа: Научная

электронная библиотека «КиберЛенинка». URL: <https://cyberleninka.ru/article/n/regulyativnye-pesochnitsy-kak-effektivnyy-mehanizm-realizatsii-tsifrovoy-povestki/viewer> (дата обращения: 28.03. 2021).

директоров (наблюдательного совета) юридического лица) судимости, отсутствие недоимки по налогам, сборам, ко всему этому добавляется, что инициатором не может быть иностранное юридическое лицо, вместе с этим установление экспериментального правового режима должно привести к достижению одной или нескольких целей.

Ко всему сказанному следует добавить, что в случае осуществления деятельности инициатором режима, в области финансового рынка, могут быть установлены ограничения объема отдельных финансовых операций и общего объема финансовых операций, осуществляемых в рамках такого экспериментального правового режима, количества лиц, в отношении которых могут осуществляться эти финансовые операции в течение срока действия экспериментального правового режима.

Самым первым и самым масштабным проектом по запуску регуляторной песочницы являлся проект Управления по финансовому регулированию (Financial Conduct Authority, FCA) в Великобритании, анонсированный в 2014 и начавший работать в 2016 году.

Для одобрения участия в таком проекте субъекты были обязаны соответствовать следующим требованиям: ориентированность на рынок Великобритании; отсутствие или незначительное количество аналогичных технологических

решений; улучшение сервиса для потребителей; противоречие с действующим законодательством. Помимо этого, таким компаниям обеспечивался доступ к нормативной экспертизе и набору нормативных инструментов для облегчения тестирования, а также предоставлялись услуги кейс-оффисера, который поддерживал разработку и внедрение теста и проводил его правовое регулирование, что позволяло компаниям понять, как их инновационные бизнес-модели вписываются в нормативную базу Великобритании.

FCA определило следующие цели, которые должны быть достигнуты в рамках осуществления проекта: сокращение времени и, возможно, затрат на вывод инновационных идей на рынок; обеспечение более широкого доступа к финансированию для новаторов за счёт снижения неопределенности регулирования; обеспечение возможности тестирования большего количества продуктов и, таким образом, потенциального вывода их на рынок; обеспечение гарантий защиты прав потребителей встроенных в новые продукты и услуги.

Исходя из результатов первого года тестирования FCA выпустил отчёт³, где отметил, что около 40 % компаний, которые проходили тестирование, смогли получить инвестиции, которые в рамках отсутствия песочницы, получить они бы не смогли.

³ Regulatory sandbox lessons learned report / Financial Conduct Authority // Financial Conduct Authority: official site. 2017. Oct.

URL: <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf> (accessed: 28.03.2021).

Модель отечественного эксперимента, в большинстве своём, схожа с моделью, действующей в Великобритании, тем не менее она имеет свои особенности, предполагая более жёсткий контроль со стороны правительства и, по сравнению, строгие условия одобрения участия субъектов в осуществляемом эксперименте. Данные меры предпринимаются в целях защиты прежде всего частных интересов, а также немаловажными представляются интересы государства, как в целом, так и отдельных его институтов.

Развитие такого института в пределах Российской Федерации представляется возможным, это позволит скорректировать направление государственной политики в сфере информационного и

финансового контроля, отменить некоторые ограничения в этой области, которые затормаживают развитие цифровых технологий, обеспечить привлечение инвестиций, развитие конкуренции, стабилизации положения цифрового рынка, обеспечение прав потребителей.

Тем не менее стоит отметить, что данный опыт в российской правовой арене является первым широкомасштабным актом применения регуляторных песочниц, это сказывается в недостаточном законодательном регулировании. Так, например, не до конца остаётся решённым вопрос о том, какие именно ограничения смогу избегать субъекты экспериментального режима, какими конкретными органами будет осуществляться регулирование проекта и т. д.

Список литературы

1. Куклина Е .А. «Регулятивные песочницы» как эффективный механизм реализации цифровой повестки // Большая Евразия: Развитие, безопасность, сотрудничество. 2019. С. 265–268. Режим доступа: Научная электронная библиотека «КиберЛенинка». URL: <https://cyberleninka.ru/article/n/regulyativnye-pesochnitsy-kak-effektivnyy-mehanizm-realizatsii-tsifrovoy-povestki/viewer>.
2. Regulatory sandbox lessons learned report / Financial Conduct Authority // Financial Conduct Authority: official site. 2017. Oct. URL: <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf>.

Vadim A. Chepurnov
Student,
Saratov State Law Academy
(Saratov, Russian Federation)
v.chep9717@yandex.ru

Scientific supervisor – A. S. Anisimova, PhD (Law), Senior Lecturer of the Department of Information Law and Digital Technologies

**REGULATORY «SANDBOXES» ON THE TERRITORY OF THE RUSSIAN
FEDERATION: LEGAL REGULATION AND PROSPECTS FOR
APPLICATION IN DOMESTIC LAW**

Abstract: This paper is devoted to the consideration of regulatory sandboxes, which until now remain without detailed legal regulation. Their content, purpose, and prospects for implementation in Russia are analyzed. The article focuses on the problems that make it difficult to consider regulatory sandboxes within the framework of Russian law.

Keywords: regulatory sandboxes, experimental legal regimes, digital innovations, digital market, legal entity.

Раздел II

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ, ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ, РОБОТОТЕХНИКА

УДК 343.1

Реховский Александр Фёдорович

Кандидат юридических наук, доцент,
заведующий кафедрой правосудия, прокурорского надзора и
криминалистики,
Дальневосточный федеральный университет
(г. Владивосток, Российская Федерация)
rekhovskiy.af@dvfu.ru

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УГОЛОВНОМ ПРОЦЕССЕ КИТАЯ

Аннотация: В статье изложен взгляд автора на произошедшие изменения в практике уголовного судопроизводства Китая, прежде всего на активное внедрение «Шанхайской интеллектуальной вспомогательной системы рассмотрения уголовных дел» (Система 206), разработанной в 2017 году. Автор дает оценку результатов судебной реформы КНР в сфере уголовного судопроизводства, главные особенности этого процесса, на примере создания и внедрения в следственную и судебную практику новых стандартов доказывания, модели «умного допроса».

Ключевые слова: искусственный интеллект, инновации, уголовное судопроизводство, судебное разбирательство, стандарты доказывания.

Для цитирования:

Реховский А. Ф. Использование искусственного интеллекта в уголовном процессе Китая // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 69–77.

За последнее десятилетие в Китае были приняты беспрецедентные меры по модернизации судебной системы с использованием искусственного интеллекта.

Как справедливо отмечает С. В. Гольман, Центральным комитетом Коммунистической партии Китая декларировано создание социалистической страны с китайской спецификой при верховенстве права, управлении государственными делами в условиях верховенства права, судебной беспристрастности,

научной обоснованности и универсального правопорядка. Разработка судебной реформы, ее осуществление и оценка результатов, с учетом как процедуры принятия нормативно-правовых актов, так и стратифицированного характера организационной структуры судов, дуализмом руководства судами, исходя из концепции народной судебной власти для народа, проводятся под контролем Центрального комитета Коммунистической партии Китая и

Всекитайского собрания народных представителей, а также при активном участии Верховного народного суда КНР¹.

За короткое время в Китае был проведен ряд экспериментов и пилотных проектов по использованию искусственного интеллекта в судебной системе. «Уже сегодня Китай достиг поразительных успехов в цифровизации экономики, производства, общественно-социальных институтов и права. Уникальный опыт цифровизации права и правовых институтов КНР представляет одну из самых актуальных тем исследования»².

В январе 2017 года Комиссия по политическим и правовым вопросам при Центральном комитете Коммунистической партии Китая – функциональное подразделение, которое руководит и управляет работой в области политики и права, направляя и контролируя соответствующие органы власти, такие как полиция, прокуратура, суд, тюрьма и т. д., – приняла решение о проведении исследований и разработке системы программного обеспечения для продвижения реформы системы уголовного судопроизводства в Китае.

Такое стратегическое решение имеет решающее значение для укрепления верховенства права в Китае, поскольку он является пионером глубокого применения

искусственного интеллекта в судебной сфере, который имеет большое значение для развития судебной системы Китая, правосудия и цивилизации³.

Шанхайский высокий народный суд был учрежден в качестве первого пилотного проекта реформы судебной системы Китая. Он взял на себя ведущую роль в продвижении реформы и добился положительных результатов. Он создал воспроизводимый и популярный «Шанхайский опыт» для реформы национальной судебной системы. Результатом проекта стало создание интеллектуальной системы. Эта система упрощенно называется «Система 206» или «Проект 206», т. к. шестого февраля 2017 года Шанхайский высокий народный суд взял на себя миссию первопроходца в реформировании судебной системы Китая.

Ранее китайские суды в течение нескольких лет разрабатывали открытые платформы судебной информации, в частности, в том, что касается публикации судебных документов и информации в Интернете.

С 2013 года в Китае появилась первая единая государственная Открытая база судебных решений (China Judgements Online).

Сегодня практически все судебные документы, подготовленные китайскими судами, публикуются на

¹ См.: Гольман С. В. Оптимизация судостройства как направление судебной реформы Китая: некоторые аспекты // Право и практика. 2018. №. 3. С. 131.

² Непейвода Н. Правосудие на кончиках пальцев: опыт КНР // Закон.ру. URL: https://zakon.ru/blog/2020/05/02/pravosudie_n

[a_konchikah_palcev_opyt_knr_83633](#) (дата обращения: 07.03.2021).

³ См.: Cui Y. Artificial Intelligence and Judicial Modernization. Springer, 2020. <https://doi.org/10.1007/978-981-32-9880-4> (accessed: 10.03.2021).

этом сайте. По состоянию на февраль 2020 года на этом сайте насчитывалось более 81,5 млн. судебных документов, представляющих собой крупнейшее в мире онлайн-хранилище судебных документов⁴. Кроме того, на этой платформе существуют еще три вебсайта, на которых размещена информация о судебном процессе, информация об исполнении судебных решений и прямая трансляция судебных слушаний на всех уровнях в режиме реального времени. Эти четыре информационные платформы превратились в крупнейший в мире пул ресурсов данных о судебных процессах. Все суды в Китае (включая 3250 судов, 9277 трибуналов и 39 морских судов) подключены к централизованной платформе SPC по управлению большими данными и обслуживанию. Данные по судебным делам собираются в режиме реального времени. Платформа автоматически обновляется каждые пять минут с помощью системы обработки информации, распространяемой по всей стране. Она обеспечивает полный охват, конвергенцию и доступность судебных данных по всей стране и подлежит строгому контролю и проверке качества данных. Местные суды или органы власти не имеют возможности приукрашивать или манипулировать статистическими данными, представляемыми на

централизованную национальную платформу. Кроме того, централизованная платформа осуществляет сбор, хранение и управление данными о сотрудниках судебных органов, судебных делах, управлении и исследовании судов на всех уровнях⁵.

Этот этап можно оценивать как подготовительный и необходимый для реализации Шанхайского проекта, т. к. искусственный интеллект имеет три элемента: базу данных, экспертные знания и операционную систему, обрабатывающую информацию.

«Система 206» имеет формальное название «Шанхайская интеллектуальная вспомогательная система для уголовных дел по реализации судебной реформы, ядром которой является судопроизводство». Ключевым моментом является термин «вспомогательная система», в котором заключается направление исследований и разработок.

Как отмечал Ядунь Цунь – председатель Шанхайского высокого народного суда и руководитель проекта в своем выступлении на интернет-вебинаре в Шанхайском политико-юридическом университете с докладом на тему «Применение искусственного интеллекта в уголовном правосудии КНР» 24.09.2020: «Прежде всего, нужно развеять недоразумение, что машина

⁴ См.: <http://wenshu.court.gov.cn>. Некоторые категории документов (а именно, дела, связанные с национальной безопасностью, правонарушениями несовершеннолетних, разводами и опекой над детьми) не предаются гласности. Информация, касающаяся личной жизни и коммерческой

тайны (кроме имен сторон), также редактируется в некоторых документах.

⁵ См.: Zou M. «Smart courts» in China and the future of personal injury litigation // Journal of Personal Injury Law (forthcoming). 2020. 11 Mar.

самостоятельно рассматривает дела. Здесь я хочу подчеркнуть: Шанхайская «Система 206» – это интеллектуальный помощник, не выполняет процесс самостоятельно. Раскрою этот вопрос в трех пунктах:

1) Особенности правосудия ограничивают использование искусственного интеллекта (далее – ИИ). ИИ может служить только помощником в рассмотрении дел. Судебной деятельности присущи беспристрастность, открытость, личная явка и т. д. Эти качества, особенно личная явка, определяют, что субъектами судебной деятельности могут быть только люди, а не ИИ.

2) Уровень развития ИИ определяет его статус вспомогательной системы. В настоящее время ИИ находится на начальном уровне, так называемом этапе слабого искусственного интеллекта, его способности пока ограничены. А судебная деятельность – это сложная деятельность, для которой нужны знания, квалификации и жизненные опыты судей, прокуроров, следователей. А ИИ не может размышлять и рассуждать как сотрудники правоохранительных и судебных органов, поэтому он не может заменить людей в рассмотрении дел. Он способен оценивать доказательства, а право на вынесение приговора сохраняется за судьями.

3) Взаимодействие человека и машины для улучшения вспомогательной системы по рассмотрению дел. Применение ИИ в области правосудия требует взаимодействия человека и машины и

межпрофильного сотрудничества. Только тесное сочетание закономерностей и особенностей правосудия со свойствами искусственного интеллекта на данном этапе развития позволяет эффективно использовать этот технологический инструмент на пользу правосудию. «Система 206» – это интеллектуальный помощник судей, прокуроров и полицейских».

Для создания «Системы 206» была сформирована научно-исследовательская группа – команда из более чем 700 человек. В ее состав входили: 1) профильная бригада судей – более 220 человек; 2) из прокуратуры – более 80 человек; 3) из полиции – более 100 человек; 4) из других судебных органов – более 10 человек, а также техническая бригада из IT-компании IFLYTEK – более 305 человек.

Первая версия «Системы 206» была создана всего за 156 дней к лету 2017 года. В настоящее время уже введена в эксплуатацию версия 3.0.

Применение вспомогательных технологий искусственного интеллекта в ходе судебного процесса осуществляется следующим образом.

По мере продолжения судебного процесса Система 206 будет автоматически идентифицировать, выбирать и отображать (на экранах зала суда) доказательственные материалы. В зале заседаний «умного» суда в ходе судебного разбирательства обычно используются следующие три функции.

1) Интеллектуальное распознавание речи: Система 206 может мгновенно и эффективно преобразовывать речь в запись

судебного заседания.

2) Интеллектуальный захват информации: Система использует такие технологии, как интеллектуальный захват элементов дела, распознавание и понимание голосовой информации и т. д. для автоматического захвата и отображения соответствующих доказательств в соответствии с вопросами и ответами подсудимого, прокурора и судьи.

3) Интеллектуальное отображение доказательств: с функциями отображения доказательств, проверки доказательств, просмотра цепочки доказательств и судебного решения, а также речевых и словесных доказательств, Система может отображать соответствующие материалы в зале суда, такие как дефекты доказательств и противоречия доказательств, обнаруженные в ходе судебного разбирательства.

Благодаря комбинированному взаимодействию этих трех функций в режиме реального времени обеспечивается интеллектуальная поддержка всего процесса судебного разбирательства.

После двух лет усилий, третья версия «Шанхайской интеллектуальной вспомогательной системы рассмотрения уголовных дел» была доступна онлайн с декабря 2018 года, что позволяет рассматривать все уголовные дела в Шанхае в режиме онлайн – от поиска, расследования, одобрения ареста, пересмотра, обвинения, судебного процесса, осуждения, до замены наказания и условно-досрочного

освобождения, представляя собой прорыв в глубоком применении технологии искусственного интеллекта в судебном разбирательстве.

Система 206, имеющая 26 функций, получила в Китае 6 прав интеллектуальной собственности.

Ее четыре отличительные функции заключаются в следующем:

(1) Стандарты доказывания и руководство по правилам доказывания. Эта функция предоставляет сотрудникам, работающим с делами, стандартизированные, оцифрованные и проверенные руководства по сбору и выявлению доказательств, которые легко понять и следовать им, с тем чтобы предотвратить заметные проблемы в этой процедуре, такие как отсутствие единообразно применяемых стандартов доказательств среди органов безопасности, прокуратуры и судов, нестандартное ведение дел, и т. д.

(2) Исследование доказательств. Система 206 может рассматривать, проверять и контролировать как единичные доказательства, так и цепочки доказательств по всему делу, и напоминать следователям, занимающимся рассмотрением дел, и сотрудникам правоохранительных органов о проблемах, связанных со своевременным представлением доказательств, с тем чтобы фактические доказательства по делам, находящимся в расследовании, рассмотрении и преследовании, могли выдержать проверку закона.

(3) Руководство по проведению допроса с ключевыми элементами. Со

своими моделями допроса/взаимодействия для различных типов дел, Система 206 может обеспечить руководство для сотрудников полиции во время допроса. Кроме того, она может помочь своевременно выявлять противоречия в признательных показаниях, чтобы гарантировать полноту, законность и точность протоколов допросов.

(4) Интеллектуальная помощь в судебном разбирательстве. Благодаря использованию искусственному интеллекту и других высокотехнологичных средств для оказания помощи в судебном разбирательстве Система 206 может обеспечить «установление фактов по делу в суде» и «определение доказательств в суде» с тем, чтобы реально осуществлять обоснование судебных разбирательств и защищать право истца на действия, а также право людей знать, участвовать, выражать свое мнение, осуществлять надзор и т. д.

Учитывая тему конференции и ее научную направленность, полагаем необходимым более подробно остановиться на вспомогательной системе «Умного допроса» для устранения ложных устных показаний и обеспечения подлинности и достоверности протокола допроса.

По мнению разработчиков Системы 206, на практике существует необоснованное доверие к признательным показаниям подозреваемого, что является важной причиной появления ошибочных обвинений.

Исследователи задались вопросом: «Как искоренить пытки,

давление и ложное признание на допросе при предоставлении достаточной свободы следователям для расследования преступления?» Эта проблема существует каждой стране. Каждое правоохранительное учреждение полагается на допрос и рассматривает его как один из наиболее эффективных инструментов расследования преступлений и обнаружения доказательств, позволяющих доказать виновность подозреваемых. Это выявляет риск – чрезмерное доверие к признательным показаниям может привести к судебной несправедливости.

Для решения этой мировой проблемы была разработана модель «Допроса по ключевым точкам». Поэтапно были сделаны следующие шаги.

Шаг 1: на основе ключевых фактов, ключевых моментов и навыков постановки вопроса, обобщенных профессионалами в этой области, формируется графа знаний для допроса по ключевым моментам.

Шаг 2: в Систему 206 была встроена модель «допроса по ключевым точкам» с массивными записями допросов в базах данных в качестве образцов для машинного обучения.

С помощью этой модели Система 206 может автоматически предлагать и направлять сотрудников правоохранительных органов, работающих с делами во время допроса, для выявления фактов по делу. С помощью этой функции сотрудники, работающие с делами, могут проводить хорошо структурированный допрос и запись, основанные на ключевых моментах

факта; вычленять устные заявления и своевременно обнаруживать в них противоречащие моменты, чтобы избежать отсутствия деталей допроса, вызванного отсутствием у них опыта, а также обеспечить полноту, законность и точность записей допроса.

Практическое значение «Умного допроса» в следующем.

Во-первых, «Умный допрос» повышает квалификацию должностных лиц по использованию доказательств и обеспечивает достоверность, точность и полноту показаний. Эта система указывает элементы допроса, по обстоятельствам дела, перечисляет важные пункты проведения допроса, предотвращает ошибки следователи из-за нехватки опыта, обеспечивает достоверность и точность и полноту показаний.

Во-вторых, «Умный допрос» (аудио- и видеозапись всего процесса, отслеживание и надзор за полным ходом процесса допроса) обязывает оперативников соблюдать законы при допросе, предотвращает получение ложных признательных показаний с помощью пыток, что гарантирует не только правдивость и законность допроса, но и права подозреваемых.

Ранее нами отмечалось, что в ходе реформы уголовного процесса в Японии в 2016 году было введено положение об обязательной видеофиксации допросов при

расследовании тяжких преступлений⁶. Но в данном случае технологии использования искусственного интеллекта не используются.

Можно сказать, что «Умный допрос» Системы 206 – революция в допросе Китая. Это большой скачок от традиционных методов допроса (включая понятие, методы и технологии) к модернизации процедуры допроса в целом. Это результаты внедрения новых технологий в судебной сфере.

Достижение применения модели «Умного допроса». К концу декабря 2019 года эта система была полностью внедрена в деятельность Шанхайской полиции. С января 2019 г. по июнь 2020 г. в Шанхае, при помощи этой системы были составлены более миллиона протоколов допроса.

Можно сказать, что развитие и применение этой Системы занимает лидирующие позиции в мире⁷.

Несмотря на значительный успех Шанхайская «Система 206» не произвела впечатления на многих судей судов первой инстанции, которые ее тестировали. Сложность в формулировке критериев определения важности той или иной части данных также означает, что «вполне возможно, что уникальный элемент, имеющий определяющее влияние на исход дела, будет отфильтрован системой [Шанхай 206] во время обработки данных и процесса отбора»⁸. Иными словами, абсолютно

⁶ См.: Реховский А. Ф. Современная реформа уголовного процесса Японии // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 1. С. 9–15.

⁷ См.: Cui Y. Artificial Intelligence and Judicial Modernization. Springer, 2020. <https://doi.org/10.1007/978-981-32-9880-4> (дата обращения: 10.03.2021).

⁸ Zhang F., Zheng H. Dashuju Shidai Rengong Zhineng Fuzhu Liangxing de Dingwei Qianjing

надежного алгоритма по анализу и проверки доказательств по уголовному делу пока создать не удалось. Именно поэтому Система 206 имеет вспомогательное значение. Окончательное решение выносит судья-человек, а не Система.

Представляется, что китайский опыт модернизации судебной системы заслуживает самого пристального внимания. К сожалению, информации об этом пока недостаточно. Отчасти этот недостаток можно объяснить тем, что научные публикации об этом выходят в свет на китайском языке.

Несмотря на отдельную критику «Системы 206» нельзя не учитывать и другие китайские проекты, такие как «Smart-суды» и «Мобильный суд», «Умная прокуратура», «Умная полиция» и другие, которые вызывают общее признание мировой общественности в том, что «Китай – законодатель моды в авторитарном мире, и необычно даже то, что среди других юрисдикций... его суды вполне могут "прыгать" в будущее "компьютеризированного судейства"»⁹.

Список литературы

1. Гольман С. В. Оптимизация судоустройства как направление судебной реформы Китая: некоторые аспекты // Право и практика. 2018. №. 3. С. 130–135.
2. Непейвода Н. Правосудие на кончиках пальцев: опыт КНР // Закон.ру. URL: https://zakon.ru/blog/2020/05/02/pravosudie_na_konchikah_palcev_opyt_knr_83633.
3. Реховский А. Ф. Современная реформа уголовного процесса Японии // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. №.1. С. 9–15.
4. Cui Y. Artificial Intelligence and Judicial Modernization. Springer, 2020. 224 p.
5. Liebman B. Mass Digitization of Chinese Court Decisions: How to Use Text as Data in the Field of Chinese Law / B. Liebman [et al.] // Journal of law and courts (forthcoming 2020).
6. Zhang F. Dashuju Shidai Rengong Zhineng Fuzhu Liangxing de Dingwei Qianjing ji Fengxian Fangkong (大数据时代人工智能辅助量刑的定位、前景及 风险防控) [Navigation, Prospects, and Risk Control of Sentencing Assistance by Artificial Intelligence in the Big Data Age] / F. Zhang, H. Zheng // Social sciences in Guangxi 92, 96 (2019).
7. Zou M. «Smart courts» in China and the future of personal injury litigation // Journal of Personal Injury Law (forthcoming). 2020. 11 Mar.

ji Fengxian Fangkong (大数据时代人工智能辅助量刑的定位、前景及 风险防控) [Navigation, Prospects, and Risk Control of Sentencing Assistance by Artificial Intelligence

in the Big Data Age] // Social sciences in Guangxi 92, 96 (2019).

⁹ Liebman B. Mass Digitization of Chinese Court Decisions: How to Use Text as Data in the Field of Chinese Law / B. Liebman [et al.] // Journal of law and courts (forthcoming 2020).

Alexandr F. Rekhovskiy

PhD (Law), Associate Professor, Head of the Department of Justice, Prosecutorial
Supervision and Criminalistics,
Far Eastern Federal University
(Vladivostok, Russian Federation)
rekhovskiy.af@dvfu.ru

**USE OF ARTIFICIAL INTELLIGENCE IN CHINESE CRIMINAL
PROCEDURE**

Abstract: The article outlines the author's view on the changes that have occurred in the practice of criminal proceedings in China, especially the active implementation of the «Shanghai Intellectual Assisted Criminal Procedure System» (System 206), developed in 2017. The author assesses the results of the PRC judicial reform in criminal proceedings, the main features of this process, with the example of the creation and implementation in the investigative and judicial practice of new standards of evidence, the model of «smart interrogation».

Keywords: artificial intelligence, innovation, criminal procedure, court proceedings, standards of proof.

Бахтеев Дмитрий Валерьевич
Кандидат юридических наук, доцент,
доцент кафедры криминалистики,
Уральский государственный юридический университет
(г. Екатеринбург, Российская Федерация)
dmitry.bakhteev@gmail.com

ОНТОЛОГИЧЕСКИЕ ОСНОВЫ РАЗРАБОТКИ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ АНАЛИЗА, ПРОГНОЗИРОВАНИЯ И ПРЕДУПРЕЖДЕНИЯ РИСКОВ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ*

Аннотация: В статье рассматриваются онтологические основы для интеллектуальной системы, обеспечивающей физическую безопасность индивида, в частности, система угроз (рисков) безопасности, источники сигналов об угрозах и их характеристики, субъекты защиты, принципы и пределы разработки такого программного обеспечения.

Ключевые слова: интеллектуальная система, предупреждение рисков, физическая безопасность, геоинформационная система.

Для цитирования:

Бахтеев Д. В. Онтологические основы разработки интеллектуальной системы анализа, прогнозирования и предупреждения рисков физической безопасности // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 78–86.

Одним из направлений цифровизации общества является использование интеллектуальных систем раннего обнаружения факторов, нарушающих безопасность человека, общества и государства. В данной статье речь пойдёт об онтологических и технологических аспектах разработки экспертной интеллектуальной системы анализа,

прогнозирования и предупреждения рисков физической безопасности для индивида на примере исследования, осуществляемого в рамках проекта¹, разрабатываемого ООО «Цифра» (участник Сколково).

Подобные проекты уже находят свою реализацию, как на государственном уровне, так и силами коммерческих организаций. Так,

* Исследование выполнено при поддержке Российского фонда фундаментальных исследований в рамках научного проекта 18-29-16001 «Комплексное исследование правовых, криминалистических и этических аспектов, связанных с разработкой и функционированием систем искусственного интеллекта» и проекта «Экспертная платформа для анализа и прогнозирования рисков физической безопасности».

¹ Проект «Экспертная платформа для анализа и прогнозирования рисков физической безопасности» (Грант Фонда содействия инновациям № 86ГСИЦТС10-D5/61818 от 17.09.2020 г.).

следует упомянуть такие проекты как City.Risks², SafeNet, Kaspersky Safe Kids, Где мои дети, Kidslox, Norton Family Parental Control, ESET Parental Control. Вполне заметно, что значительная часть перечисленных проектов ориентирована на обеспечение безопасности конкретной группы граждан, а именно детей.

Любое определение безопасности зависит от отраслевой принадлежности его автора. Так, обладателем или носителем этого состояния может быть физическое или юридическое лицо, их группа (отрасль), информационная система, общество, государство и т. п. В области охраны труда это может означать отсутствие угроз нанесения повреждений в процессе производства³. Для психологов – высокая степень защиты от психологических и эмоциональных угроз⁴. Общим для всех указанных подходов является принцип защищённости от чего-либо, то есть каждому определению безопасности де-факто должно предшествовать установление определённых рисков, опасностей, угроз. Соответственно, категории безопасности дифференцируются в зависимости от субъекта защиты (например, индивида или профессиональной группы), по

объекту угрозы (например, жизни и здоровью) и по источнику угрозы. Таким образом, физическая безопасность, являющаяся предметом настоящей статьи, сводится, по нашему мнению, к ограждению индивида от причинения ему физического вреда или ограждение его от угроз причинения физического вреда, вызванного различными факторами: природными, техногенными, социогенными. Другим аспектом этого понятия, также достойным упоминания, является обусловленность защищённости интересами индивида⁵, то есть риски или угрозы могут варьироваться в зависимости от интересов человека, обусловленных его возрастом, мировоззрением, физическими возможностями и прочими факторами.

Согласно ст. 22 Конституции Российской Федерации, каждому её гражданину гарантируется право на личную неприкосновенность. Вместе тем неиллюзорными являются риски нарушения этого права. Поэтому каждый четвертый россиянин (25 %) не чувствует себя в безопасности в «чужих» районах своего города, а каждый пятый – не чувствует себя в безопасности в своем районе (21 %) и даже на дворе своего дома (18 %) ⁶.

² Avoiding and mitigating safety risks in urban environments// CORDIS: EU research results. URL: <https://cordis.europa.eu/project/id/653747> (accessed: 20.04.2021).

³ Physical Safety // The free dictionary. URL: <https://legal-dictionary.thefreedictionary.com/Physical+Safety> (accessed: 20.04.2021).

⁴ What is physical safety? // Your experiences matter. URL: <https://yourexperiencesmatter.co>

[m/learning/safe-spaces/physical-safety/what-is-physical-safety/](https://learning/safe-spaces/physical-safety/what-is-physical-safety/)(accessed: 20.04.2021).

⁵ Безопасность человека // МЧС России: официальный сайт. URL: <https://www.mchs.gov.ru/ministerstvo/o-ministerstve/terminy-mchs-rossii/term/3386> (дата обращения: 20.04.2021).

⁶ Как россияне оценивают качество городской среды и динамику ее изменения // ВЦИОМ: официальный сайт. 2020. URL: <https://wciom.ru/analytical->

Разумеется, в большей мере это относится к рискам, существующим в условиях большого города как основного места проживания людей в условиях продолжающейся урбанизации.

В наиболее широком смысле такие риски могут быть дифференцированы по их источнику на социогенные (как, правило, криминального характера), техногенные (например, разрушение строительных конструкций, выброс в атмосферу токсичных веществ, пожары и т. д.), природного характера (наводнения, эпидемии и т. д.).

К примеру, в российских городах риск стать жертвой преступного посягательства в целом сохраняется: ежегодно совершается 2 млн преступлений, жертвами которых становятся 1,65 млн человек⁷, четыре из пяти преступлений (79,7 %) совершаются в городах, причем более трети – в общественных местах (на улицах, площадях, в парках и скверах и т. д.).

Треть (32 %) россиян убеждены, что уровень преступности за

последние 10 лет вырос⁸, 27 % не ощущают снижения уровня преступности, при этом лишь 9 % россиян имеют средства самообороны и лишь 6% носят их с собой⁹. Поэтому возрастает значение проактивных инструментов (в т. ч. рекомендательных информационных сервисов, работающих в режиме реального времени) для снижения рисков физической безопасности для горожан и членов их семей.

Риски физической безопасности для жителей городов социогенными рисками не исчерпываются. Так, половина всех чрезвычайных ситуаций, 58 % пожаров, 75 % ДТП происходят в городах¹⁰, а также большая часть других техногенных аварий на сетях (электро-, газо-, теплосети).

С точки зрения хронологических характеристик риски можно разделить на статические и динамические.

Первые связаны с определённой территорией и, меняя свою интенсивность в зависимости от отдельных временных интервалов

reports/analiticheskii-doklad/sreda-kotorayanas-formiruet-kak-rossiyane-ocenivayut-kachestvo-gorodskoj-sredy-i-dinamiku-ee-izmeneniya (дата обращения: 20.04.2021).

⁷ Характеристика состояния преступности в Российской Федерации за январь–декабрь 2019 года // Министерство внутренних дел Российской Федерации: официальный сайт. URL: <https://media.mvd.ru/files/application/1748898> (дата обращения: 20.04.2021).

⁸ Полиция: отношение и оценки работы // Фонд «Общественное мнение»: официальный сайт. URL: <https://fom.ru/Bezopasnost-i-pravo/14228> (дата обращения: 20.04.2021).

⁹ Самооборона и оружие / Фонд «Общественное мнение». URL: <https://fom.ru/Bezopasnost-ipravo/14172>.

¹⁰ Государственный доклад «О состоянии защиты населения и территорий Российской Федерации от чрезвычайных ситуаций природного и техногенного характера в 2018 году» / МЧС России, ФГБУ ВНИИ ГОЧС (ФИЦ). М.: 2019, 344 с. Режим доступа: МО «Посёлок Стрельна»: официальный сайт. URL: https://mo-strelna.ru/upload_files/articles/2019/06/GosDoklad_po_2018_godu_Print.pdf; Показатели состояния безопасности дорожного движения // ГИБДД: официальный сайт. URL: <http://stat.gibdd.ru/> (дата обращения: 20.04.2021).

(например, времени суток), в целом сохраняются в течение продолжительного времени. Примером источника такого риска может служить мусорные площадки и полигоны твёрдых бытовых отходов.

Динамические риски, в свою очередь, существуют в течение непродолжительного времени и, как правило, на ограниченной территории. Иллюстрацией динамических рисков являются массовые мероприятия.

Следует учитывать, однако, что представленные риски могут пересекаться, в том числе быть вложенными друг в друга: стая бродячих собак (динамический источник риска) может существовать на территории полигона твёрдых бытовых отходов (статический источник риска).

Применительно к интеллектуальным системам данный аспект таксономической системы важен как ориентир для формата информирования конечного пользователя: статические риски следует отображать в интерфейсе постоянно, либо через фильтры полей (в геоинформационной системе), а динамические – при их появлении, в том числе, например, в виде push- или sms-сообщений на мобильных устройствах. Так, именно динамическим угрозам природного характера посвящено sms-информирование Министерства по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий. В Таблице 1 представлена более развёрнутая система статических и динамических рисков.

Таблица 1.

Пример	Тип	Тип риска по источнику	Геолокационные и хронологические характеристики
Нападение на улице	Ситуация, локация	Социогенные (криминальные)	
Террористический акт, КТО	Ситуация, локация	Социогенные (криминальные)	
Массовое мероприятие	Ситуация, локация	Социогенные	
Железная дорога, ж/д переезды	Локация	Техногенные	
Заброшенные здания	Локация	Техногенные / социогенные	
Стройки	Локация	Техногенные / социогенные	
Вокзалы, ж/д станции	Локация	Техногенные / социогенные	
Порты	Локация	Техногенные / социогенные	
Набережные и береговые зоны	Локация	Социогенные	
Рынки	Локация	Социогенные	
Ломбарды	Локация	Социогенные	
Алкомаркеты	Локация	Социогенные	

Заправки	Локация	Социогенные	
Бары	Локация	Социогенные	
Гаражные комплексы	Локация	Социогенные	
Улицы без освещения	Локация	Социогенные	
Парковочные зоны	Локация	Социогенные	
Пригороды, дачи	Локация	Социогенные	
Свалки, полигоны ТБО	Локация	Техногенные / социогенные	
Автобусный транспорт	Локация	Техногенные / социогенные	
Ж/д транспорт	Локация	Техногенные / социогенные	
Водный транспорт	Локация	Техногенные / социогенные	
Инциденты в сети электроснабжения	Ситуация, локация	Техногенные	
Инциденты в сети водоснабжения	Ситуация, локация	Техногенные	Динамический
Нападения диких животных	Ситуация, локация	Природные	Динамический
Аварии на технологических предприятиях	Ситуация, локация	Техногенные	Динамический
ДТП	Ситуация, локация	Техногенные / социогенные	Динамический
Природные явления	Ситуация, локация	Природные	Динамический
Эпидемии	Ситуация, локация	Природные	Динамический

Указанные в Таблице 1 локации характеризуются либо изолированностью от мест нахождения людей, либо напротив – повышенной вероятностью нахождения в таких местах криминализированных элементов, а также трудностью или фактической невозможностью обращения за помощью к неопределённому кругу лиц (например, прохожим).

С точки зрения интеллектуальной обработки сигналов о рисках, последние можно разделить по степени их достоверности на высоко-, средне- и низковоероятные. Любая система, получающая сигналы, характеризующие внешнюю среду, подвержена также информационным

шумам. Оценка достоверности сигнала напрямую зависит от типа угрозы, возможности реакции на угрозу государственных органов исполнительной власти, самого формата сигнала (сообщения в СМИ, в социальных сетях, через интерфейс мобильного приложения и т. д.) и множества иных факторов. Именно определение этой характеристики детерминирует эффективность функционирования интеллектуальной системы по обеспечению физической безопасности.

Источники сигналов, в свою очередь могут быть дифференцированы на происходящие их органов государственной власти, либо от граждан.

В первом случае задействуются различные системы мониторинга определённых событий в реальном времени, к примеру, подразделения ГИБДД активно используют государственную систему экстренного реагирования «Эра-Глонасс», промышленная эксплуатация которой началась с 2015 года. Она включает в себя навигационно-информационную платформу, сеть передачи данных и сеть сотовой связи по принципу «виртуального оператора») и устройства (автомобильная система в терминах стандарта), устанавливаемые в автомобили. Данные из этой системы поступают в АИС ОСАГО и в страховые компании. «Эра-Глонасс» связана как с системами сотовой, так и спутниковой связи, в том числе зарубежными аналогичными системами, например, с европейской eCall и казахстанской Эвак.

К информации, поступающей от граждан и служащей источником данных для интеллектуальной системы, относятся сообщения пользователей в социальных сетях, открытых группах в мессенджерах и данные геолокации пользователей.

Разумеется, в обоих случаях для корректного использования сведений о реализации рисков кластеры информации должны быть сопоставлены с моделью территории, на которой реализован риск. Это обуславливает необходимость задействования массивов пространственных данных (геоинформационных систем), включающих также отдельные

сведения об объектах инфраструктуры (например, проект Open Street Map).

Ключевыми принципами функционирования интеллектуальной системы, ориентированной на обеспечение безопасности, почерпнутыми как из сущности применяемых технологий (таких как машинное (глубокое) обучение, геоинформационные, сетевые технологии и пр.), так и из нормативно-этической сферы, являются:

1. Простота интеграции в существующую цифровую инфраструктуру – возможность внедрения «поверх» существующих систем сбора, хранения и использования данных за счёт использования динамической онтологии безопасности, позволяющей достичь интероперабельности данных, полученных из разнородных источников.

2. Гибкость разработки и использования за счёт микросервисной архитектуры.

3. Масштабируемость за счёт использования открытого программного интерфейса приложения (API), развитие экосистемы разработчиков и пользователей за счёт развития настраиваемых клиентских приложений.

4. Обеспечение безопасности и сохранности персональных данных пользователей.

5. Адаптивность в условиях существования динамических рисков.

6. Учёт индивидуальных поведенческих и психологических

особенностей субъекта использования программного обеспечения в целях.

7. Информационно-техническое взаимодействие с органами государственной власти.

8. Соблюдение режима законности, в первую очередь, при сборе и хранении данных.

9. Точность аналитических и прогностических выводов системы.

10. Использование либо открытых, либо санкционированных источников информации для обучения и настройки системы. В большинстве случаев современные интеллектуальные системы основаны на технологиях машинного обучения и искусственных нейронных сетях. Не вдаваясь глубоко в сущность данных технологий, необходимо указать, что для обучения и верификации результатов обучения требуется массив больших данных, в рассматриваемой ситуации – данных, содержащих структурированные или неструктурированные сведения о ситуациях риска физической безопасности. Такие данные могут включать, как было указано ранее, данные о транспортной обстановке, массовых мероприятиях, природных и техногенных происшествиях, пользовательские данные (геолокация и сообщения), массивы пространственных данных об объектах инфраструктуры (Open Street Map). Рассмотрим специфику обработки сообщений пользователей социальных сетей как источника входных данных для интеллектуальной системы.

Такие данные должны в первую очередь отбираться из открытых источников, желательно, как можно

более специфического характера: группа городских новостей менее полезна, чем группа городских новостей о дорожно-транспортных происшествиях. Следует учитывать, что пользовательские сообщения могут содержать нерелевантную или повреждённую информацию. В последнем случае сообщение можно считать достоверным, однако без дополнительного подтверждения невозможным для использования, к примеру, сведения о сущности инцидента указаны, однако информация о его месте не указана, либо указана неконкретно. В отдельных случаях (к примеру, при анализе ДТП) точный адрес может не требоваться (достаточным будет указание улицы). Учитывая глубину возможных комбинаций сообщения об одном и том же факте, требуется составление словаря (тезауруса): как для описания сущности риска, так и для указания его локации. Разметка сообщений по критериям их достоверности и соответствия требованиям полноты описания риска в большинстве случаев должна осуществляться ассессором-человеком.

Разработка такой системы неизбежно осложняется совокупностью разнородных внутренних рисков – пределов технологии, к которым можно отнести:

1. Риски технического характера: трудности получения доступа или сбора данных для обучения, недостаточные результаты итоговой точности работы системы.

2. Риски конфликтного характера: отказ органов государственной власти, организаций

и физических лиц предоставлять информацию.

3. Риски этического характера: отсутствие доверия со стороны конечных пользователей.

4. Риски правового характера: прямое нарушение законодательства, либо нарушение компетенции государственных органов, нарушение режима работы с данными ограниченного доступа (в том числе персональными данными), в том числе и вследствие изменения законодательства.

Представленные риски являются обобщёнными и при корректном планировании разработки, апробации и внедрения системы могут быть предотвращены.

Наиболее очевидными пользователями анализируемого программного обеспечения являются

лица, имеющие ограниченную осведомлённость о геолокации и сущностной характеристике отдельных рисков: в первую очередь, это дети (в этом случае пользователем может быть родитель) и лица, постоянно в конкретном городе не проживающие (в том числе туристы).

Таким образом, разработка интеллектуальной системы, ориентированной на информирование граждан с целью их защиты от угроз физической безопасности обязательно должна включать в себя изучение онтологических основ соответствующей технологии, включающих в себя изучение таких угроз (рисков), системы источников сигналов о них, субъектах защиты, принципов и пределов разработки такого программного обеспечения.

Список литературы

1. Государственный доклад «О состоянии защиты населения и территорий Российской Федерации от чрезвычайных ситуаций природного и техногенного характера в 2018 году» / МЧС России, ФГБУ ВНИИ ГОЧС (ФЦ). М.: 2019, 344 с. Режим доступа: МО «Посёлок Стрельна»: официальный сайт. URL: https://mo-strelna.ru/upload_files/articles/2019/06/GosDoclad_po_2018_godu_Print.pdf.

2. Как россияне оценивают качество городской среды и динамику ее изменения // ВЦИОМ: официальный сайт. 2020. URL: <https://wciom.ru/analytical-reports/analiticheskii-doklad/sreda-kotoraya-nas-formiruet-kak-rossiyane-oczenivayut-kachestvo-gorodskoj-sredy-i-dinamiku-ee-izmeneniya>.

3. Полиция: отношение и оценки работы // Фонд «Общественное мнение»: официальный сайт. URL: <https://fom.ru/Bezopasnost-i-pravo/14228>.

4. Самооборона и оружие / Фонд «Общественное мнение». URL: <https://fom.ru/Bezopasnost-i-pravo/14172>.

5. Physical Safety // The free dictionary. URL: <https://legal-dictionary.thefreedictionary.com/Physical+Safety>.

Dmitry V. Bakhteev

PhD (Law), Associate Professor of the Department of Criminalistics,
Ural State Law University
(Yekaterinburg, Russian Federation)
dmitry.bakhteev@gmail.com

**ONTOLOGICAL BASIS FOR THE DEVELOPMENT OF AN
INTELLIGENT SYSTEM FOR ANALYSIS, PREDICTION AND PREVENTION
OF PHYSICAL SECURITY RISKS**

Abstract: The article discusses the ontological foundations for an intelligent system that ensures the physical security of an individual, in particular, a system of security threats (risks), sources of signals about threats and their characteristics, protection subjects, principles and limits of the development of such software.

Keywords: intelligent system, risk prevention, physical security, geographic information system.

УДК: 343.1

Евстратова Юлиана Айратовна

Кандидат юридических наук, доцент, профессор кафедры уголовного процесса и криминалистики факультета (командного),
Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации
(г. Санкт-Петербург, Российская Федерация)
yuliana130682@mail.ru

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: В статье рассмотрены технологические основы и возможности применения систем искусственного интеллекта в правоохранительной деятельности Росгвардии. Описаны методы и сущность искусственного интеллекта. Исследованы подходы к таксономии систем искусственного интеллекта. Определяются основные признаки искусственных нейронных сетей, в частности способность к ситуационному адаптивному обучению, выявлению неочевидных связей и закономерностей.

Ключевые слова: Росгвардия, искусственный интеллект, информационное взаимодействие, виды и свойства информации, информационный ресурс, государственная безопасность, общественная безопасность, искусственные нейронные сети.

Для цитирования:

Евстратова Ю. А. Перспективы применения технологий искусственного интеллекта в деятельности войск национальной гвардии Российской Федерации // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 87–93.

В октябре 2019 года президент России Владимир Владимирович Путин утвердил Национальную стратегию развития искусственного интеллекта до 2030 года. В Национальной стратегии развития искусственного интеллекта указаны приоритетные научные задачи — обеспечение ускоренного развития

искусственного интеллекта в Российской Федерации, проведение научных исследований в области искусственного интеллекта, повышение доступности информации и вычислительных ресурсов для пользователей, совершенствования системы подготовки кадров в этой области¹.

¹ О развитии искусственного интеллекта в Российской Федерации (вместе с

«Национальной стратегией развития искусственного интеллекта на период до

Приоритетные направления развития и использования технологий искусственного интеллекта определяются в России с учетом национальных целей и стратегических задач, определенных Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»². Вышеуказанные, нормативно-правовые акты подчёркивают колоссальную государственную и общественную важность данных разработок в современной России.

Что же понимается под искусственным интеллектом?

Искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную

инфраструктуру, программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений³.

Одной из основных целей изучения искусственного интеллекта для войск национальной гвардии Российской Федерации является обеспечение государственной и общественной безопасности, защиты прав и свобод человека и гражданина. Применение искусственного интеллекта в войсках национальной гвардии позволит эффективно и оперативно решать поставленные задачи, например такие как:

1) участие в охране общественного порядка, обеспечении общественной безопасности;

2) охрана важных государственных объектов, специальных грузов, сооружений на коммуникациях в соответствии с перечнями, утвержденными Правительством Российской Федерации;

3) участие в обеспечении режимов чрезвычайного положения, военного положения, правового режима контртеррористической операции⁴.

2030 года»): указ Президента РФ от 10.10.2019 № 490 // СПС «КонсультантПлюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 01.01.2021).

² О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: указ Президента Российской Федерации от 7 мая 2018 г. № 204 // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/>

[/cons/cgi/online.cgi?req=doc&base=LAW&n=335184&fld=134&dst=100017,0&rnd=0.84658](http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=335184&fld=134&dst=100017,0&rnd=0.84658)

71413771306#0732290413048083/ (дата обращения: 01.01.2021).

³ О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): указ Президента РФ от 10.10.2019 № 490 // СПС «КонсультантПлюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 01.01.2021).

⁴ О войсках национальной гвардии Российской Федерации: федеральный закон от 03.07.2016 № 226-ФЗ (ред. от 02.12.2019)

Искусственный интеллект «на службе» Росгвардии позволит эффективно управлять большим объёмом данных, элементарных кластеров информации и способен реализовать важные фундаментальные операции: постановка задачи – запоминание – обучение – использование знаний.

В настоящее время назрела необходимость применения искусственных нейронных сетей при реализации задач Росгвардии.

Искусственные нейронные сети – это математические модели, а также их программные или аппаратные реализации, построенные по принципу организации и функционирования биологических нейронных сетей – сетей нервных клеток живого организма. Это понятие возникло при изучении процессов, протекающих в мозге, и при попытке смоделировать эти процессы⁵.

Искусственные нейронные сети являются важнейшей составляющей технологий машинного обучения. Последние представляют набор методов решения поставленной задачи не напрямую (путём жёсткой алгоритмизации), а путём обучения.

Работа искусственной нейронной сети во многом схожа с обучением человека, мозг которого по сути представляет естественную нейронную сеть.

На первом этапе разработки системы искусственного интеллекта на базе искусственной нейронной сети происходит формирование датасета –

базы данных, которая будет использована для обучения. Элементы датасета (чаще всего это графические изображения или текстовая информация) должны быть взаимно непротиворечивы и представлять класс объектов как можно более полно. К примеру, если нейросеть ориентирована на точное распознавание лиц, автомобильных номеров, оружия, то в датасете должны присутствовать данные объекты, тогда распознавание произойдет. Далее осуществляется выбор или создание алгоритма обучения искусственной нейронной сети. Алгоритм обучения в числе прочего может содержать условия окончания обучения, порядок предъявления примеров обучающей выборки, коэффициенты погрешностей, количество возможных ошибок перед сменой установок и т. д. Сеть должна содержать правила, по которым должны происходить обобщение или дифференциация элементом датасета. Также искусственная нейронная сеть может быть настроена либо на постоянное обновление алгоритмов обучения, либо на самостоятельное развитие по заранее заданным параметрам (эволюцию).

При обучении нейросетей используются следующие (итерационные) алгоритмы:

1) алгоритмы локальной оптимизации с вычислением частных производных первого порядка, градиентный алгоритм (метод

(с изм. и доп., вступ. в силу 01.01.20) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_200506 (дата обращения: 01.01.2021).

⁵ Искусственная нейронная сеть // Академик. URL: <https://dic.academic.ru/dic.nsf/ruwiki/13889> (дата обращения 12.01.2021).

наискорейшего спуска), методы с одномерной и двумерной оптимизацией целевой функции в направлении антиградиента, метод сопряженных градиентов, методы, учитывающие направление антиградиента на нескольких шагах алгоритма;

2) алгоритмы локальной оптимизации с вычислением частных производных первого и второго порядка: метод Ньютона, методы оптимизации с разреженными матрицами Гессе, квазиньютоновские методы, метод Гаусса-Ньютона, метод Левенберга-Марквардта и др.;

3) стохастические алгоритмы оптимизации: поиск в случайном направлении, метод Монте-Карло (численный метод статистических испытаний);

4) алгоритмы глобальной оптимизации (задачи глобальной оптимизации решаются с помощью перебора значений переменных, от которых зависит целевая функция)⁶.

Использование «обученных» искусственных нейронных сетей в правоохранительной деятельности Росгвардии, на наш взгляд является своевременной необходимостью. Искусственные нейросети современного поколения могут реализовывать следующие, типы операций: распознавание, предсказание, классификация.

1. Распознавание — определение необходимых признаков

в исследуемых данных, к примеру идентификация внешности человека по анатомическим и функциональным признакам; идентификация автомобилей; идентификация огнестрельного и холодного оружия, правоустанавливающих документов и т. д.

В соответствии с Указом Президента РФ от 30.09.2016 г. № 510 «О Федеральной службе войск национальной гвардии Российской Федерации»⁷ Росгвардия является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере деятельности войск национальной гвардии Российской Федерации, в сфере оборота оружия, в сфере частной охранной деятельности, в сфере частной детективной деятельности и в сфере вневедомственной охраны.

К приоритетным задачам Росгвардии относятся, в том числе, задачи по нормативно-правовому регулированию в установленных сферах деятельности и по организации участия войск национальной гвардии в охране общественного порядка и обеспечении общественной безопасности. В рамках реализации вышеуказанных функций необходимо полноценное распознавание и продуктивная идентификация,

⁶ Обучение нейронной сети // Портал знаний об искусственном интеллекте neuronus.com. URL: <https://neuronus.com/theory/nn/238-obucheniya-nejronnoi-seti.html> (дата обращения 12.01.2021).

⁷ О Федеральной службе войск национальной гвардии Российской Федерации: указ Президента РФ от 30 сентября 2016 г. № 510 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_205384/ (дата обращения: 01.01.2021).

использование искусственного интеллекта позволит быстрее и эффективнее реализовать вышеуказанные функции.

Распознавание криминального поведения в общественном месте, и идентификация лица, нарушающего общественный порядок, является основным видом мыслительной деятельности при участии сотрудников и военнослужащих Росгвардии в охране общественного порядка. Использование «обученных» нейронных сетей позволит автоматически выявлять признаки систематических нарушений общественного порядка, за которые виновные лица понесут административное наказание.

Программное обеспечение, используемое в охране общественного порядка, позволит определять внешние анатомические признаки правонарушителей и преступников (цвет глаз и волос, форму лица и головы).

В рамках деятельности Росгвардии, предлагаем внедрить использование спутниковых систем для участия в охране общественного порядка. Искусственный интеллект может проводить анализ создания и провокации опасных ситуаций, нарушающих права и свобода граждан и лиц, пребывающих на территории Российской Федерации. Внедрение искусственного интеллекта в спутниковые системы, на наш взгляд, реально повысит эффективность, в том числе обеспечения режимов чрезвычайного положения, правового режима контртеррористической операции.

В деятельности войск национальной гвардии Российской Федерации, в сфере оборота оружия, частной охранной деятельности, частной детективной деятельности и в сфере вневедомственной охраны, предлагаем внедрить консультации с чат-ботом. Думается, применение чат-ботов для консультирования граждан, позволит гражданам получить исчерпывающую информацию по интересующему вопросу, а сотрудников Росгвардии, выполняющих консультационное сопровождение, направить на выполнение других важных функций и перераспределить их должностные обязанности.

Чат-бот – это виртуальный собеседник, программа-собеседник – программа, которая выясняет потребности пользователей, а затем помогает удовлетворить их. Автоматическое общение с пользователем ведется с помощью текста или голоса. Чат-бот, будет вести коммуникацию от лица сотрудника Росгвардии, с целью упростить онлайн-общение (предоставить актуальную информацию в наиболее оперативные сроки), используется как альтернатива переписке с живым сотрудником.

Думается, есть реальная необходимость в цифровизации и воинских частей национальной гвардии. Целесообразно создать единую информационную систему во всех округах, внедрить видеоаналитику с распознаванием лиц, электронный документооборот на всей территории России, системы контроля передвижения и

эксплуатации транспорта на территории воинской части.

Следующий тип операции нейронных сетей – это предсказание.

2. Предсказание – определение будущего состояния определённой информационной системы или отдельных её показателей, к примеру, роста или снижения показателей преступности.

В этом случае предъявляется совокупность статистических данных, на основании анализа которых система должна сделать предположение о будущем состоянии и вариантах развития источников данных. На основе технологий искусственного интеллекта, машинного зрения и методов анализа больших данных можно реализовывать учебные программы для курсантов, обучающихся в военных учреждениях войск национальной гвардии при подготовке курсантов в дальнейшем к участию в охране общественного порядка, к обеспечению безопасности массовых мероприятий, несанкционированных митингов и т. д. Искусственный интеллект может оценить место скопления людей, дислокацию сотрудников, их количество, агрессивность толпы, создание опасных моментов и ситуаций для жизни и здоровья людей. Операция «предсказание» позволит искусственному интеллекту вырабатывать наиболее эффективную стратегию для сотрудников Росгвардии по противодействию и

ликвидации криминального поведения с минимальным применением спецсредств и минимальным количеством возможных пострадавших граждан.

На наш взгляд, важный и необходимый тип операции нейронных сетей, который необходимо внедрить в работу войск, – это классификация данных.

3. Классификация – распределение данных по группам согласно заданным параметрам, к примеру, отнесение оружия к огнестрельному, холодному, гражданскому, боевому и т. д. Классификационные типы операций уже внедряются в деятельность правоохранительных органов России.

Думается, в настоящее время, необходимо использовать нейросети при реализации контроля за соблюдением обязательных требований при проведении мероприятий по контролю за деятельностью юридических лиц, осуществляющих выполнение работ (услуг) по хранению и по торговле гражданским и служебным оружием (его основных частей) и патронов (их составных частей). В настоящее время назрела необходимость создания федеральной единой электронной современной системы учета гражданского оружия.

Анализируя вышеизложенное, считаем, что использование искусственного интеллекта позволит более эффективно реализовывать функции и задачи Росгвардии.

Список литературы

1. Искусственная нейронная сеть // Академик. URL: <https://dic.academic.ru/dic.nsf/ruwiki/13889>.
2. Обучение нейронной сети // Портал знаний об искусственном интеллекте neuronus.com. URL: <https://neuronus.com/theory/nn/238-obucheniya-nejronnoi-seti.html>.

Yuliana A. Evstratova

PhD (Law), Associate Professor, Professor of the Department of Criminal Procedure and Forensics of the Faculty (Command),
Saint Petersburg Military Order of Zhukov Institute of the National Guard of the Russian Federation
(Saint Petersburg, Russian Federation)
yuliana130682@mail.ru

PROSPECTS FOR THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE ACTIVITIES OF THE NATIONAL GUARD TROOPS OF THE RUSSIAN FEDERATION

Abstract: The article considers the technological foundations and the possibilities of using artificial intelligence systems in the law enforcement activities of the Russian Guard. The methods and nature of artificial intelligence are described. Approaches to the taxonomy of artificial intelligence systems are investigated. The main features of artificial neural networks are determined, in particular, the ability to situational adaptive learning, to identify non-obvious connections and patterns.

Keywords: Rosgvardiya, artificial intelligence, information interaction, types and properties of information, information resource, state security, public security, artificial neural networks.

Зазулин Анатолий Игоревич

Кандидат юридических наук, старший юрист юридической фирмы INTELLECT,
(г. Екатеринбург, Российская Федерация)
a.zazulin@intellectmail.ru

ОЦЕНКА ДОКАЗАТЕЛЬСТВ, ПОЛУЧЕННЫХ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация: Статья посвящена исследованию технологий искусственного интеллекта с позиции оценки доказательств, которые могут быть получены посредством их использования. На основе уже существующих тенденций по цифровизации и применению ИИ в других областях человеческой деятельности, автор делает предположение о том, что в ближайшем будущем данная технология станет активно использоваться и в судопроизводстве, в том числе при расследовании преступлений. Единых подходов к оценке доказательств, полученных с помощью ИИ, в мире не выработано, что приводит к судебным ошибкам, вызванным чрезмерным доверием к технологиям – приводятся примеры таких случаев в Дании и США. Это влечет за собой необходимость уже сейчас начать разработку правил судебной оценки результатов деятельности ИИ. Для этого, следовательно, необходимо понять механизм обучения ИИ – краткий обзор данного процесса представлен в настоящей статье. На основе анализа особенностей машинного и глубоко обучения ИИ делается ряд выводов относительно критериев оценки достоверности полученных такими ИИ сведений. В статье выделяются следующие проблемные аспекты, которые влияют на оценку результатов работы ИИ в судопроизводстве: качество входящих наборов больших данных, использованных для обучения; правильность «лейблизации» или «тегирования» указанных данных; обоснованность тестового набора «правильных ответов»; прозрачность механизма обучения ИИ. На этой основе автором выводится ряд основных критериев использования и оценки ИИ: прозрачность и обоснованность данных и методик, использованных для обучения ИИ; прозрачность механизма принятия ИИ решений (что пока исключает использование ИИ, основанных на технологии нейросетей); ансамблированность программного продукта ИИ. В заключении автор противопоставляет методологию науки о больших данных, положенную в основу обучения ИИ, методологии юриспруденции: первая имеет дело с числами, показателями и измеряемыми объектами, тогда как право – с недискретными понятиями «справедливости», «равноправия» и т. д. Роль правоприменителя в данном случае – соблюсти баланс между двумя идеологиями.

Ключевые слова: судопроизводство, предварительное расследование, большие данные, искусственный интеллект, машинное обучение, глубокое обучение, нейросеть, оценка доказательств.

Для цитирования:

Зазулин А. И. Оценка доказательств, полученных в результате использования искусственного интеллекта // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 94–103.

В крупную корпорацию поступает резюме соискателя на открывшуюся вакансию. Специальный программный алгоритм на основе указанных в резюме и социальных сетях данных претендента создает отчет, в котором содержатся рекомендации HR-менеджеру: подходит ли соискатель на должность, обладает ли он необходимыми качествами и опытом, какие вопросы необходимо задать на собеседовании.

Торговая сеть или стриминговый сервис анализируют интернет-активность пользователя и с помощью новейших программ предугадывают его желания и предпочтения, предлагая именно тот продукт, который будет наиболее интересен покупателю.

Все эти примеры – уже реальность. Темы искусственного интеллекта, больших данных и машинного обучения являются в настоящее время наиболее обсуждаемыми как в обществе, так и в науке. И хотя соответствующая область науки существует уже более 50 лет, только сейчас об ИИ заговорили настолько серьезно и обстоятельно: технология перестала быть обитателем исключительно научно-фантастических

произведений. Почему именно сейчас?

Нынешнее бурное развитие ИИ является результатом логичного поэтапного процесса развития информационных технологий. Первым шагом стало, естественно, изобретение компьютеров и их постоянное совершенствование – цифровой бум последнего десятилетия обусловлен уменьшением размера вычислительных устройств в соответствии с законом Мура¹. По мере уменьшения вычислителей, они становились все более доступными и удобными для приобретения и использования.

Развитие Интернета и совершенствование компьютерных процессоров являлись взаимообусловленными процессами, главным результатом совместного действия которых был рост количества людей и организаций, способных качественно и быстро обмениваться информацией.

К началу второго десятилетия XXI века количество устройств и пользователей в глобальной сети стало генерировать все больше и больше информации, причем информации, которую можно было легко зафиксировать. Впервые в истории человечества стало

¹ Закон Мура – эмпирическое наблюдение, изначально сделанное Гордоном Муром, согласно которому численность транзисторов, размещаемых на кристалле

интегральной схемы, умножается каждые 24 месяца в 2 раза. Цит. по: Аноприенко А. Я. Обобщения закона Мура // Информатика и кибернетика. 2017. № 3 (9). С. 14.

возможным мгновенно отследить действия любого человека или устройства – маршрут движения автомобиля, время и место покупок, поездки на общественном транспорте или участие в мероприятии – так как они сразу же дублировались в интернет-среде. Так появились т. н. «большие данные» («Big Data») – огромные массивы несистематизированных цифровых следов, которые можно было проанализировать и сделать на их основе соответствующие прогнозы. Возникновение больших данных и необходимость их обработки привели к необходимости стремительного совершенствования технологий ИИ. По своей сути последние представляют собой интеллектуальные методы статистического анализа и прогнозирования.

Инструменты искусственного интеллекта все больше внедряются во все сферы общественной жизни. Не стало исключением и судопроизводство: специальный софт для автоматического поиска и распознавания детской порнографии на изъятых у подозреваемого устройствах²; алгоритмы анализа

коммуникационных данных для определения статической и динамической геолокации смартфонов³; программы прогноза криминального рецидива осужденных⁴.

Не трудно предсказать тенденцию все большей имплементации таких инструментов в судопроизводство, включая предварительное расследование по уголовным делам. Их использование, таким образом, будет порождать экспоненциальный рост количества цифровых доказательств в материалах дел. Это, в свою очередь, приведет к необходимости разработки и совершенствования правил оценки цифровых доказательств, полученных в результате работы ИИ. Для этого ученым и практикам уже сейчас необходимо понимать, как работает современный ИИ.

В классическом программировании разработчик создает правила, после чего программа обрабатывает входящие данные по указанным правилам и выдает ответ. При создании ИИ компьютеру даются и данные, и ответы – его задача состоит в том, чтобы самостоятельно найти

² Искусственный интеллект в борьбе против детской порнографии // Официальный портал правительства земли Северный Рейн – Вестфалия [сайт]. URL: <https://www.land.nrw/de/pressemitteilung/kuenstliche-intelligenz-im-kampf-gegen-kinderpornographie> (дата обращения: 28.04.2021).

³ Ewald U. Volatilität digitaler Beweise - Herausforderung für die Cyber-Strafverteidigung // Rechtsanwälte für wirtschaftsstrafrecht in Kooperation [website]. URL: [https://rechtsanwaelte-wirtschaftsstrafrecht-](https://rechtsanwaelte-wirtschaftsstrafrecht-berlin.de/volatilitaet-digitaler-beweise-herausforderung-fuer-die-cyber-strafverteidigung/)

[berlin.de/volatilitaet-digitaler-beweise-herausforderung-fuer-die-cyber-strafverteidigung/](https://rechtsanwaelte-wirtschaftsstrafrecht-berlin.de/volatilitaet-digitaler-beweise-herausforderung-fuer-die-cyber-strafverteidigung/) (accessed: 28.04.2021).

⁴ Например, «COMPAS»: Christin A., Rosenblat A., Boyd D. Courts and predictive algorithms // Data & Civil rights: a new era of policing and justice. [сайт]. URL: https://datasociety.net/wp-content/uploads/2015/10/Courts_and_Predictive_Algorithms.pdf (дата обращения: 28.04.2021) или «LSI-R»: О'Нил К. Убийственные большие данные. Как математика превратилась в оружие массового поражения. М.: АСТ, 2018. С. 15.

корреляции и правила, ведущие от полученных данных к полученным ответам. Этот процесс называется «обучением», хотя более точным термином является «усвоение»⁵. После него ИИ может обрабатывать новые входящие данные, применяя самостоятельно сформулированные им при обучении правила для выдачи ответов и прогнозов.

Говоря более конкретно, обучение ИИ выглядит следующим образом: в вычислительную систему подается входящая информация в форме наборов больших данных. Каждая единица информации «лейблируется», т. е. ей дается ее дискретное описание. Например, изображение разбирается на категории количества пикселей, их цвета, концентрации пикселей в определенной части изображения. Другой пример: описание человека разделяется на отдельные признаки – метки: пол, возраст, наличие детей, статус работы и т. д. Эти «якори» являются основой последующего процесса обучения – компьютер будет находить между ними корреляции и связи, позволяющие сделать правильный прогноз.

Далее следует случайная обработка данных компьютером: вычислительные звенья дают тот или иной (случайный) ответ на поставленную задачу. Данные ответы сравниваются с тестовым набором данных – «правильными ответами».

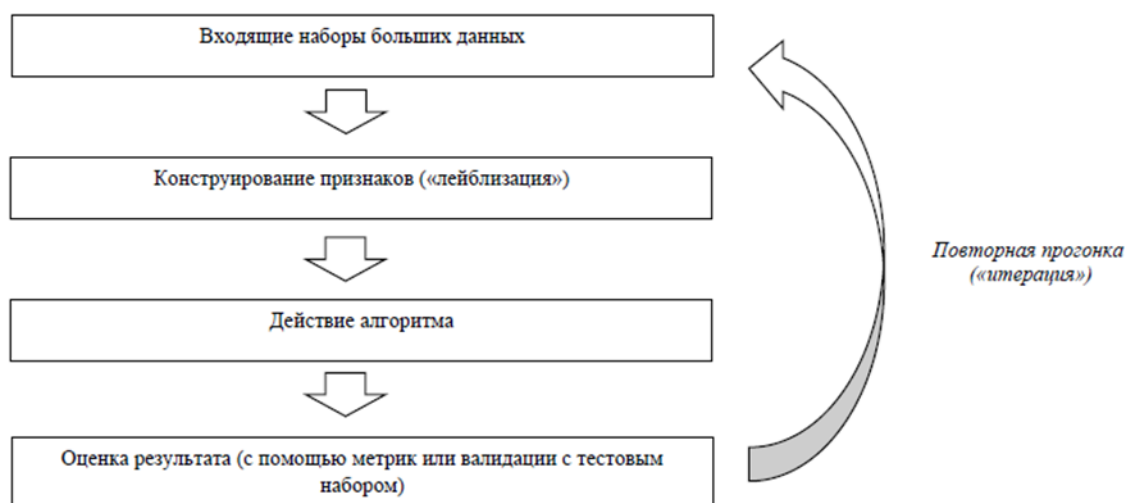
После этого вычислительные звенья ранжируются по значимости: больший показатель значимости приобретают те из них, кто правильно (хоть и случайно) ответил на поставленную задачу. Один и тот же пакет входящих данных может «прогоняться» через вычислительные звенья бесчисленное количество раз, пока точность предсказания результатов не достигнет максимального результата⁶.

Вычислительные звенья могут иметь отслеживаемую человеком относительно простую архитектуру – в таком случае мы можем говорить о простом машинном обучении. Однако они также могут быть выстроены в более сложные комплексные структуры, подразумевающие большое количество слоев. Такие структуры называются нейросетями, а машинное обучение, осуществляемое при их помощи, – глубоким обучением. Отличительной чертой глубокого обучения является проблема «черного ящика» – никто, в том числе другой ИИ, не может в точности сказать, как отдельно взятая нейросеть пришла к определенному выводу⁷.

⁵ Комментарий переводчика, или никто никого не обучает // Хабр. URL: <https://habr.com/ru/post/554150/> (дата обращения: 28.04.2021).

⁶ Ын А., Су К. Теоретический минимум по Big Data. Все, что нужно знать о больших данных. СПб.: Питер, 2019. С. 21–39.

⁷ Hutson M. AI in Action: How algorithms can analyze the mood of the masses // Science. 2017. Vol. 357, Issue 6346. P. 23.



Какие проблемы кроет в себе такой механизм образования будущих цифровых доказательств?

Искажение входящих данных. Искажение работы ИИ возможно уже на стадии входящих данных. Как было описано ранее, процедуре обучения ИИ предшествует стадия «лейблирования» изучаемых объектов. И в качестве таких ярлыков разработчиком могут использоваться те элементы, которые *хотя и позволяют улучшить точность системы, но вносят в нее значительный элемент дискриминации*. Так, при независимом анализе использующейся в США программы прогноза криминального рецидива COMPAS в качестве входных параметров учитывала расу: осужденным афроамериканского происхождения в результате анализа она рекомендовала назначить более длительные сроки наказания⁸.

Некоторым это может показаться оправданным, ведь по статистике именно эта группа людей в

США совершает большее количество преступлений. Однако в данном случае стоит учесть, что уголовный процесс всегда нацелен на анализ личности самого осужденного, распространение на него свойств всей группы людей, к которым он принадлежит, является грубым нарушением принципа презумпции невиновности.

О том, насколько важным может быть анализ критериев, введенных разработчиками ИИ на этапе входящих данных, может говорить другой пример. Представим, что одним из лейблов входящих данных стал показатель положительной кредитной истории осужденного. Разработчик, полагаясь на бытовую логику, посчитал, что люди с хорошей финансовой дисциплиной вряд ли станут рецидивистами. В итоге более длительный срок наказания может получить человек, просрочивший выплату кредита по причине нахождения под стражей по уголовному делу, в рамках которого

⁸ How We Analyzed the COMPAS Recidivism Algorithm / J. Larson, S. Mattu, L. Kirchner, J. Angwin // ProPUBLICA [website]. URL:

<https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> (accessed: 28.04.2021).

используется ИИ. Справедлива ли указанная ситуация? Сомнительно.

Более того, сами входящие данные, использованные для обучения ИИ, должны быть также достоверны, т. е. собраны из заслуживающих доверия публичных источников. В противном случае ИИ выдает логичный, но основанный на неверных данных результат («мусор на входе – мусор на выходе»).

Неправильная методика оценки результатов. Каким бы автономным не было обучение ИИ, человек играет в нем главную роль: он не только отбирает необходимые данные для обучения, но и корректирует результаты, оценивает верность данных при обучении ответов (либо вручную, либо путем отбора «правильных ответов»). Именно разработчик указывает ИИ, что является правильным, а что нет – соответственно критерии определения им «правильности» так же должны быть проверены на предмет обоснованности и соответствия правовым принципам.

Непрозрачность механизма работы ИИ. Логично предположить, что для определения достоверности полученных посредством использования ИИ доказательств, механизм образования таких доказательств должен быть прозрачен и ясен. Другими словами, субъект оценки должен иметь возможность убедиться в том, как ИИ пришел к определенному выводу – по аналогии с тем, как оценивается механизм образования классических доказательств.

Транспарентность механизма принятия решения ИИ во многих случаях нарушается самими разработчиками ИИ: ведь механизм работы ИИ и технология его обучения являются коммерческой тайной⁹. С другой стороны, раскрытие такой информации может представлять угрозу для всего правопорядка – например, в случае если соответствующий алгоритм используется полицейскими органами всей страны. Будет ли оправдан в таком случае риск раскрытия «исходного кода» назначенному судом стороннему эксперту, даже при проведении закрытого судебного заседания и предупреждении последнего об уголовной ответственности?

Другой проблемой возможного отсутствия транспарентности алгоритмов работы ИИ является уже упомянутая «проблема черного ящика». Последняя свойственна ИИ, использующим технологию глубокого машинного обучения – т. е. обучения с помощью нейросетей. Эту проблему хорошо описали специалисты Датского центра цифровых исследований: *«системы, основанные на нейронных сетях (например, в глубоком обучении), не предлагают понятного человеку объяснения предоставленных ответов. Отсутствие объяснения ... в некоторых ситуациях может быть*

⁹ Katz Y. Manufacturing an Artificial Intelligence Revolution // SSRN. 2017. URL:

<http://dx.doi.org/10.2139/ssrn.3078224> (accessed: 28.04.2021).

недопустимым, как в случае юридических решений»¹⁰.

Отметим, что именно в Дании в результате ошибки в работе программы, обрабатывавшей геолокационные данные мобильных устройств подозреваемых, в 2019 году был проведен пересмотр 10 000 уголовных дел, по итогам которого были отменены приговоры в отношении 32 осужденных. Как указывается, при первоначальном рассмотрении указанных дел, следствие и суд в большинстве случаев чрезмерно «доверяли» результатам работы программы¹¹. С ростом цифровизации риск возникновения подобных ситуаций будет только увеличиваться. Эту проблему понимают и разработчики российской Концепции развития машиночитаемого права: *«также следует учитывать, что лица, осуществляющие правоприменение, при появлении цифровых помощников, формулирующих решения конкретного дела, могут некритично полагаться на результаты его работы»*¹².

Решение указанных проблем можно найти в более комплексном подходе к разработке и обучению ИИ,

предназначенного для использования в правосудии.

Во-первых, прозрачным должен быть процесс разработки таких ИИ: в случае возникновения сомнений в достоверности ИИ-доказательств, у суда должна иметься возможность проверить все этапы обучения ИИ. В случае разработки цифровых помощников судей, принципы отбора входящих данных, построения алгоритма и формирования критериев оценки результатов должны быть вынесены на общественное обсуждение по аналогии с законопроектами. Указанные принципы должны быть научно и логически обоснованы.

Во-вторых, пока технология использования нейросетей не обеспечивает надлежащего уровня транспарентности механизма обучения ИИ, достоверность полученных с его помощью данных не может быть проверена, а значит и применена при осуществлении правосудия.

В-третьих, наибольшую степень достоверности и точности могут обеспечить только такие программные продукты, которые используют ансамблированность

¹⁰ Verifiable and Robust AI // DIREC: Digital Research Centre Denmark [website]. URL: <https://direc.dk/verifiable-and-robust-ai/> (accessed: 28.04.2021).

¹¹ Ewald U. Volatilität digitaler Beweise - Herausforderung für die Cyber-Strafverteidigung // Rechtsanwälte für wirtschaftsstrafrecht in Kooperation [website]. URL: <https://rechtsanwaelte-wirtschaftsstrafrecht-berlin.de/volatilitaet-digitaler-beweise-herausforderung-fuer-die-cyber-strafverteidigung/> (accessed: 28.04.2021).

¹² Проект концепции развития машиночитаемого права // Официальный портал Иновационного центра и Фонда «Сколково» (ВЭБ.РФ) [сайт]. URL: https://sk.ru/media/documents/30.12.2020._%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82_%D0%BA%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D0%B8%D0%B8_%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%BE%D1%87%D0%B8%D1%82%D0%B0%D0%B5%D0%BC%D0%BE%D0%B3%D0%BE_%D0%BF%D1%80%D0%B0%D0%B2%D0%B0.pdf (дата обращения: 28.04.2021).

нескольких ИИ при принятии решения: такая концепция предполагает объединение в одной программе нескольких ИИ, обученных в разных парадигмах: окончательное решение программы выводится при сопоставлении результатов этих независимых ИИ методом большинства или среднего показателя в зависимости от поставленных задач¹³. Таким образом, для соответствия высоким стандартам правосудия, только ансамблированные ИИ могут быть использованы в отправлении правосудия.

В заключение хотелось бы обратить внимание на следующее. Технологии ИИ построены на методах математического анализа и статистических данных. Эти методы предназначены для работы с числами и показателями, их основной и естественной задачей является повышение эффективности соответствующей системы. При этом любая математическая модель не обладает абсолютной точностью – погрешности неустранимы при любом ее применении к «живой» материи. Для математика и специалиста в области анализа данных предпочтительным было бы наиболее

прагматическое и эффективное решение проблемы: например, пожертвовать одним невиновным, чтобы обеспечить общее снижение преступности. Таковы методология данных отраслей человеческого знания.

Не стоит забывать, что право (каким бы оно ни было технологичным) имеет дело не с показателями, а с реальными людьми, а также с тем, что зачастую нельзя измерить – справедливостью, равноправием и защищенностью. Для него гораздо большим злом является отпустить подозреваемого, чем осудить невиновного.

Эти два полярных подхода в настоящее время начинают все больше соприкасаться друг с другом в эпоху тотальной цифровизации, когда мы стоим на пороге внедрения ИИ в систему правосудия. Уравновесить их, синтезировав в единый мощный инструмент – вот актуальнейшая и сложнейшая задача правоприменителя. Роль последнего, таким образом, только возросла, а ответственность перешла на новый уровень. В этом дивном новом мире решающее значение играет человек, а не машина. Впрочем, так было всегда.

Список литературы

1. Аноприенко А. Я. Обобщения закона Мура // Информатика и кибернетика. 2017. № 3 (9). С. 14–23.
2. О’Нил К. Убийственные большие данные. Как математика превратилась в оружие массового поражения. М.: АСТ, 2018. 340 с.

¹³ Существуют и иные модели принятия общего решения ансамблированными ИИ, помимо указанных в тексте настоящей статьи. Подробнее: Ын А., Су К.

Теоретический минимум по Big Data. Все, что нужно знать о больших данных. СПб.: Питер, 2019.

3. Ын А. Теоретический минимум по Big Data. Все, что нужно знать о больших данных / А. Ын, К. Су. СПб.: Питер, 2019. 208 с.
4. Christin A. Courts and predictive algorithms / A. Christin, A. Rosenblat, D. Boyd // Data & Civil rights: a new era of policing and justice. URL: https://datasociety.net/wp-content/uploads/2015/10/Courts_and_Predictive_Algorithms.pdf.
5. Ewald U. Volatilität digitaler Beweise - Herausforderung für die Cyber-Strafverteidigung // Rechtsanwälte für wirtschaftsstrafrecht in Kooperation. URL: <https://rechtsanwaelte-wirtschaftsstrafrecht-berlin.de/volatilitaet-digitaler-beweise-herausforderung-fuer-die-cyber-strafverteidigung/>.
6. How We Analyzed the COMPAS Recidivism Algorithm / J. Larson, S. Mattu, L. Kirchner, J. Angwin // ProPUBLICA URL: <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>.
7. Hutson M. AI in Action: How algorithms can analyze the mood of the masses // Science. 2017. Vol. 357, Issue 6346. P. 23.
8. Katz Y. Manufacturing an Artificial Intelligence Revolution // SSRN. 2017. URL: <http://dx.doi.org/10.2139/ssrn.3078224>.

Anatolii I. Zazulin

PhD (Law), Senior lawyer at INTELLECT Law Firm
(Yekaterinburg, Russian Federation)
a.zazulin@intellectmail.ru

EVALUATION OF EVIDENCE GENERATED BY THE ARTIFICIAL INTELLIGENCE

Abstract: The article is devoted to the study of artificial intelligence technology from the perspective of evaluating the evidence that can be obtained through its use. Based on current trends in digitalization and the use of AI in other areas of human activity, the author assumes that in the near future this technology will be actively used in court proceedings, including the investigation of crimes. There is no uniform approach to the evaluation of evidence generated by AI, which leads to judicial errors caused by excessive reliance on technology - examples of such cases in Denmark and the US are given. This entails the need to start developing rules for judicial evaluation of AI results now. To do this therefore it is necessary to understand the mechanism of AI learning – a brief overview of this process is presented in this article. Based on the analysis of machine learning and deep learning features of AI, a number of conclusions are made regarding the criteria for assessing the validity of information obtained by such AI. The article highlights the following problematic aspects that affect the evaluation of AI performance in judging: the quality of incoming big data sets used for training; the correctness of the «labelling» or «tagging» of said data; the validity of the test set of «correct answers»; the transparency of the AI training mechanism. On this basis the author derives a number of main criteria for the use and evaluation of AI: transparency and validity of the data and techniques used for AI training; transparency of the AI decision-making mechanism

(which excludes the use of AI based on neural network technology); ensemblicity of the AI software product. The author concludes by contrasting the methodology of big data science underlying AI training with the methodology of jurisprudence: the former deals with numbers, indicators and measurable objects, whereas law deals with non-discrete concepts of «justice», «fairness» etc. The role of the enforcer in this case is to strike a balance between the two ideologies.

Keywords: judicial proceedings, preliminary investigation, big data, artificial intelligence, machine learning, deep learning, neural network, evidence evaluation.

Коваленко Ксения Евгеньевна

Кандидат юридических наук, доцент юридического института, доцент,
Алтайский государственный университет
(Барнаул, Российская Федерация)
Kovalenko1288@mail.ru

Коваленко Наталья Евгеньевна

Магистрант,
Алтайский государственный университет
(Барнаул, Российская Федерация)
4852bmh@mail.ru

**ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ИЛИ ОТОБРАЖЕНИЕ ЗАПРОСА
ОБЩЕСТВА И ПРАВА**

Аннотация: В статье рассмотрены вопросы отношения общества к искусственному интеллекту через призму правовой действительности. Искусственный интеллект утвердился в современном обществе, но действительно ли он существует или это обычная метафора, на сколько объективным и справедливым он может быть? Ответы на данные вопросы рассматриваются через призму правовой действительности.

Ключевые слова: искусственный интеллект, безопасность, интернет, общество.

Для цитирования:

Коваленко К. Е. Искусственный интеллект или отображение запроса общества и права / К. Е. Коваленко, Н. Е. Коваленко // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 104–110.

Уровень развития интеллекта отличает человека от животного, но он присущ каждому живому организму. Интеллект же непосредственно связан с эмоционально-психологическим отношением человека к окружающему его миру. Интеллектуальная деятельность человека – уникальное явление, оно включает в себя как рациональные, так и иррациональные варианты поведения, последние, в

частности, заключается в поиске нестандартных вариантов действий.

Человечество постепенно отходит от традиционных способов организации своей деятельности и постепенно аккумулируется в электронном пространстве. Цифровая трансформация, информационная безопасность, автономные устройства и искусственный интеллект, вопросы регулирования интернета вещей и электронных финансовых услуг и

электронных денег, идентификация субъектов в интернете – эти и многие подобные вопросы стали объектом пристального внимания ученых в последнее время. Вопросы соотношения права и интернета рассматривались учеными с разных сторон. Так, В. В. Архипов и В. Б. Наумов рассматривали информационно-правовые аспекты формирования законодательства о робототехнике¹, Д. В. Бахтеев – этико-правовые аспекты искусственного интеллекта², А. А. Васильев и Ж. И. Ибрагимов изучали с точки зрения регулирования робототехники и искусственного интеллекта³, Г. А. Гаджиев, Е. А. Войникас – в цифровой экономике⁴, О. П. Зайцева, Н. С. Атаманская, А. В. Гордюшина – применение искусственного интеллекта в банковской сфере⁵, М. П. Казакова – в трудовом праве⁶, Р. А.

Миннебаев рассматривал искусственный интеллект как систему правового регулирования⁷, О. В. Михайленко, Г. А. Доррер – проблемы больших данных и искусственного интеллекта в медицине⁸, А. С. Процай, М. А. Иващенко – искусственный интеллект в уголовном праве⁹; свои исследования смежным вопросам посвящали и многие другие.

Искусственный интеллект утвердился в современном обществе, но действительно ли он существует или это обычная метафора? Насколько объективным и справедливым он может быть? Каковы этические проблемы искусственного интеллекта? Уровень развития интеллекта отличает человека от животного, он присущ каждому живому организму. Интеллект же непосредственно связан с эмоционально-психологическим

искусственного интеллекта в банковской сфере // Актуальные вопросы современной экономики. 2020. № 11. С. 327–330.

⁶ Казакова М. П. Перспективы развития искусственного интеллекта в трудовом праве // Вопросы российской юстиции. 2020. № 10. С. 235–239.

⁷ Миннебаев Р. А. Искусственный интеллект как система правового регулирования // Социально-экономические и технические системы: исследование, проектирование, оптимизация. 2020. № 3 (86). С. 70–74.

⁸ Михайленко О. В., Доррер Г. А. Методологические проблемы больших данных и искусственного интеллекта в медицине // Информатизация и связь. 2020. № 6. С. 21–24.

⁹ Процай А. С. Искусственный интеллект в уголовном праве РФ // Вопросы российской юстиции. 2020. № 10. С. 412–417; Иващенко М. А. Искусственный интеллект в уголовном законодательстве России // Академическая мысль. 2020. № 4 (13). С. 62–65.

¹ Архипов В. В., Наумов В. Б. Информационно-правовые аспекты формирования законодательства о робототехнике // Информационное право. 2017. № 1. С. 19–27; Архипов В. В., Наумов В. Б. О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности // Закон. 2017. № 5. С. 157–170.

² Бахтеев Д. В. Искусственный интеллект: этико-правовые основы. Москва, 2021. 176 с.

³ Васильев А. А., Ибрагимов Ж. И. Правовое регулирование робототехники и искусственного интеллекта в европейском союзе // Российско-азиатский правовой журнал. 2019. № 1. С. 50–54.

⁴ Гаджиев Г. А., Войникас Е. А. Может ли робот быть субъектом права? (поиск правовых форм для регулирования цифровой экономики) // Право: журнал Высшей школы экономики. 2018. № 4. С. 41–48.

⁵ Зайцева О. П., Атаманская Н. С., Гордюшина А. В. Применение

отношением человека к окружающему его миру. Интеллектуальная деятельность человека уникальное явление, оно включает в себя как рациональное, так и иррациональные варианты поведения, последние, в частности, заключается в поиске нестандартных вариантов действий.

Рассмотрим сказанное через призму правовой действительности. В человеке при встрече с правом возникает особое состояние, в науке именуемым правовым чувством, это непосредственно эмоциональное выражение необходимости и справедливости определенной правовой регламентации тех или иных отношений в существующих общественных условиях. Оно содержит эмоциональную установку правомерного как должного. Оценка должного на эмоциональном уровне правосознания осуществляется с позиций интересов общностей, через категорию правовой психологии.

Естественный, природный интеллект человека мы противопоставляем искусственному интеллекту. Теперь следует обратиться к дефиниции искусственного интеллекта. Так, в доктрине П. М. Морхат рассматривает его как полностью или частично автономную самоорганизующую (самоорганизующуюся) компьютерно-аппаратно-программную виртуальную или киберфизическую, в том числе биокибернетическую, систему, наделенную/обладающую способностями и возможностями мыслить, самоорганизовываться,

обучаться, самостоятельно принимать решения и т. д.¹⁰. Наблюдаем такие характеристики как способность и возможность мыслить, самоорганизовываться, обучаться, самостоятельно принимать решения – деятельность субъектов с искусственным интеллектом направлена на автоматизацию и самостоятельность своей деятельности. Речи о иррациональности не ведется, отступить от правил такой субъект не может, что приведет к потере новых открытий и достижения в любой сфере общественной жизнедеятельности, начиная с научно-технической и заканчивая правовой, когда речь заходит о выборе правовой оценки поведения при отправлении правосудия т. д.

Искусственный интеллект тяжело внедряется в российский социум, что отчасти объясняется масштабной территорией государства. Данный фактор является одной из причин буксовки в процессе законодательного регулирования понятия и определения субъекта искусственного интеллекта, роботов и т. п. Несмотря на это он уже действует рядом с нами. Явление, существует, регламентация – нет. Существующие правовые нормы и институты не могут полностью обеспечить гарантии и защиту как социума, так и само искусственного интеллекта.

Прослеживается классический конфликт старого «укоренившегося» права с новой реальностью, с новыми потребностями общества. Социум, привыкнув к обычаю своего

¹⁰ Морхат П. М. Искусственный интеллект: правовой взгляд. Москва, 2017. С. 69.

поведения, очень тяжело и медленно адаптируется к новейшей цифровизационной вершине. Как укоренившееся поведение, так и соответствующие ему правовые знания, навыки у социума классического подхода.

В этом плане интересным представляется неоднозначность и судебной практики, например, в области трудовых споров, регламентирующая электронное взаимодействие между работником и работодателем:

1) Апелляционное определение Мосгорсуда от 22.12.2014 года по делу № 33-41638/14. Согласно материалам дела, после ознакомления с приказом об увольнении, сотрудник компании обратился в медицинское учреждение, где ему был выдан больничный лист в связи с временной нетрудоспособностью. После увольнения гражданин возражал против увольнения на том основании, что он был уволен в период нетрудоспособности. Суд установил, что в материалах нет доказательств того, что работник сообщил о своей болезни. По мнению суда, упоминание работником того факта, что он сообщил о своем заболевании по электронной почте работодателя, не может служить доказательством того, что он надлежащим образом уведомил работодателя, если нет других способов уведомления. Суд подчеркнул, что заявления работодателя при рассмотрении дела свидетельствуют о том, что адрес

электронной почты, на который сотрудник отправил сообщение, устарел и не используется в практике компании. Работодатель также заявил в суде, что работник не информировал работодателя каким-либо другим способом. Изучив материалы дела, суд пришел к выводу, что истец действовал недобросовестно, и признал увольнение законным¹¹.

2) Решение Московского городского суда от 26.06.2017 г. Согласно материалам дела, двое сотрудников были уволены в результате сокращения штата по ч. 1 п. 2 ст. 81 ТК РФ. Суд не принял во внимание доводы о том, что они были уволены в период нетрудоспособности. Он придерживался мнения, что работодатель не знал, что работники находятся на больничном. Сработали следующие соображения: судя по распечатке входящего электронного письма от руководителя отдела кадров, автоматизированная система не получала никакой информации о регистрации входящих документов за исследуемый период; показания свидетеля – главного специалиста отдела кадров показали, что листы нетрудоспособности работодателю не передавались, поэтому, суд пришел к выводу, что увольнение было законным¹².

3) Апелляционное определение Мосгорсуда от 26.05.2016 г. Работник был уволен по п. 2 ч. 1 ст. 81 ТК РФ о сокращении численности штата. Однако в день увольнения у нее был

¹¹ Апелляционное определение Мосгорсуда от 22.12.2014 года по делу № 33-41638/14 // СПС «КонсультантПлюс» (дата обращения: 17.05.2021).

¹² Решение Московского городского суда от 26.06.2017 г. // СПС «КонсультантПлюс» (дата обращения: 17.05.2021).

открыт листок временной нетрудоспособности. Поэтому она обратилась в суд с требованием признать увольнение незаконным, восстановить ее на работе и взыскать заработную плату за период вынужденного отсутствия. Суд постановил, что работница должным образом не проинформировала работодателя о своей болезни – суд не считал отправленные электронные письма доказательством этого факта¹³.

4) Определение Московского городского суда от 06.06.2017 по делу № 33-21183/2017. В данном споре директор организации уведомил сотрудников о привлечении к дисциплинарной ответственности. Подтверждением уведомления послужили следующие материалы: электронное письмо директора сотруднику; e-mail ответ сотрудника директору с отказом в исполнении; скриншот истории отчетов на сайте. Рассмотрев все указанные материалы суд считал правильным извещение сотрудника о применении в

отношении него дисциплинарного взыскания¹⁴.

Следовательно, приходим к тому, что общая категория — «искусственный интеллект», в настоящий момент не может найти свое легальное объективированное выражение. Как научное достижение, это несомненно принесет большой вклад в развитие промышленности, экономики государства, но о вторжении его в социум, в профессии, связанные с особенностью человеческого разума, естественного интеллекта, говорить еще рано. В правовой же сфере до сих пор не все нормативно-правовые акты приведены в соответствие с Конституцией РФ, существуют пробелы, устранять которые необходимо для здорового и правильного правового регулирования общества и нельзя допускать разногласия в таких важнейших для законности и порядка законах, как Уголовный кодекс, Уголовно-процессуальный кодекс и другие.

Список литературы

1. Архипов В. В. Информационно-правовые аспекты формирования законодательства о робототехнике / В. В. Архипов, В. Б. Наумов // Информационное право. 2017. № 1. С. 19–27.
2. Архипов В. В. О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности / В. В. Архипов, В. Б. Наумов // Закон. 2017. № 5. С. 157–170.
3. Бахтеев Д. В. Искусственный интеллект: этико-правовые основы. Москва, 2021. 176 с.

¹³ Апелляционное определение Мосгорсуда от 26.05.2016 г. // СПС «КонсультантПлюс» (дата обращения: 17.05.2021).

¹⁴ Определение Московского городского суда от 06.06.2017 по делу № 33-21183/2017// СПС «КонсультантПлюс» (дата обращения: 17.05.2021).

4. Васильев А. А. Правовое регулирование робототехники и искусственного интеллекта в европейском союзе / А. А. Васильев, Ж. И. Ибрагимов // Российско-азиатский правовой журнал. 2019. № 1. С. 50–54.
5. Гаджиев Г. А. Может ли робот быть субъектом права? (поиск правовых форм для регулирования цифровой экономики) / Г. А. Гаджиев, Е. А. Войникас // Право: журнал Высшей школы экономики. 2018. № 4. С. 41–48.
6. Зайцева О. П. Применение искусственного интеллекта в банковской сфере / О. П. Зайцева, Н. С. Атаманская., А. В. Гордюшина // Актуальные вопросы современной экономики. 2020. № 11. С. 327–330.
7. Иващенко М. А. Искусственный интеллект в уголовном законодательстве России // Академическая мысль. 2020. № 4 (13). С. 62–65.
8. Казакова М. П. Перспективы развития искусственного интеллекта в трудовом праве // Вопросы российской юстиции. 2020. № 10. С. 235–239.
9. Миннебаев Р. А. Искусственный интеллект как система правового регулирования // Социально-экономические и технические системы: исследование, проектирование, оптимизация. 2020. № 3 (86). С. 70–74.
10. Михайленко О. В. Методологические проблемы больших данных и искусственного интеллекта в медицине / О. В. Михайленко, Г. А. Дорпер // Информатизация и связь. 2020. № 6. С. 21–24.
11. Морхат П. М. Искусственный интеллект: правовой взгляд. Москва, 2017. 257 с.
12. Процай А. С. Искусственный интеллект в уголовном праве РФ // Вопросы российской юстиции. 2020. № 10. С. 412–417.

Ksenia E. Kovalenko

PhD (Law), Associate Professor of Law Institute, Associate Professor,
Altai State University
(Barnaul, Russian Federation)
4852bmh@mail.ru

Natalia E. Kovalenko

Graduate student,
Altai State University
(Barnaul, Russian Federation)
4852bmh@mail.ru

ARTIFICIAL INTELLIGENCE OR DISPLAYING A REQUEST OF SOCIETY AND LAW

Abstract: The article deals with the issues of society's attitude to artificial intelligence through the prism of legal reality. Artificial intelligence has established itself in modern society, but does it really exist or is it a common metaphor? And how objective and fair can it be? Answers to these questions are considered through the prism of legal reality.

Keywords: artificial intelligence, security, internet, society.

УДК 347.77.025

Шарапа Инга Александровна

Кандидат юридических наук, доцент,
доцент кафедры гражданско-правовых дисциплин,
Белорусский государственный экономический университет
(г. Минск, Республика Беларусь)
inga1166000@gmail.com

АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ К РЕГУЛИРОВАНИЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация: В статье проводится гражданско-правовое исследование и осмысление феномена искусственного интеллекта, состояния и особенностей его правового регулирования, привлечения внимания общественности к потенциалу задействования технологии искусственного интеллекта, необходимости создания правовой базы для использования динамично развивающихся достижений информационно-коммуникационных технологий.

Ключевые слова: искусственный интеллект, робототехника, право интеллектуальной собственности.

Для цитирования:

Шарапа И. А. Анализ существующих подходов к регулированию искусственного интеллекта // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 111–115.

Современные компьютерно-программные технологии и технологии робототехники продолжают стремительно, очень интенсивно развиваться. Одной из наиболее перспективных, потенциально применимых во многих сферах общественных отношений и уже применяемых в ряде сфер и при этом наиболее неоднозначных технологий являются как раз технологии искусственного интеллекта. Использование современных систем искусственного интеллекта упрощает поиск решения сложнейших комплексных задач в различных областях человеческой деятельности. При этом, правовые

аспекты, связанные с обеспечением правовой охраны и принадлежностью прав на результаты, создаваемые системами искусственного интеллекта, не решаются так просто, как может показаться на первый взгляд, и в последнее время стали популярным предметом дискуссий среди ученых и практиков, поднимающих вопросы, которые пока еще не получили полноценной научной проработки и освещения. Проблема усугубляется практически полным отсутствием законодательного регулирования указанных вопросов как на международном и региональном уровнях, так и в национальных

юрисдикциях большинства стран мира.

Устоявшегося общепризнанного определения понятия «искусственный интеллект» сегодня не существует.

Существует множество разнообразных подходов к интерпретации понятия искусственного интеллекта. Тот или иной подход к определению понятия искусственного интеллекта в существенной степени зависит (и будет зависеть) от целей разработки такого понятия и его дальнейшего применения.

В науке имеется большое разнообразие дефиниций и объяснений понятия «искусственный интеллект». Некоторые авторы дают искусственному интеллекту широкое определение компьютеризированной системы, демонстрирующей поведение, которое широко воспринимается как требующее наличия разума. Другие авторы определяют искусственный интеллект как систему, способную рационально решать сложные проблемы или предпринимать надлежащие действия для достижения своих целей независимо от условий. Третьи – выводят интерпретацию искусственного интеллекта через понятие машин, выполняющих функции, которые требуют интеллектуальных способностей при их реализации человеком. Принимая во внимание и обобщая содержащиеся в научных исследованиях монографиях, диссертациях и статьях, в нормативных правовых актах, официальных документах, заявлениях, рекомендациях интерпретации понятия

«искусственный интеллект» под термином «искусственный интеллект» можно рассматривать систему алгоритмов для ЭВМ, способную копировать некоторые процессы человеческого интеллекта, путем накопления и анализа информации, полученной в результате обработки загруженных данных и (или) полученной из считывания информации об окружающей среде, с целью выработки оптимального решения о совершении действия для достижения поставленной человеком задачи, обладающую способностями обучения, адаптации и некоторой степенью креативности, как способности принимать альтернативное решение, когда первоначальное не предоставляет возможность достичь поставленной цели.

Благодаря впечатляющему развитию технологий за последние 10 лет современные роботы способны выполнять работу, которую раньше могли выполнять только люди. Более того, благодаря развитию конкретного функционала, позволяющего роботам действовать автономно и осуществлять когнитивные процессы, например, способность роботов обучаться на своем опыте и принимать самостоятельные решения, роботы все больше и больше становятся похожи на агентов, которые могут взаимодействовать со своей средой и вносить в нее значительные изменения. В таком контексте одним из важнейших вопросов становится вопрос о правовой ответственности за вред, причинённый действием робота.

До недавнего времени развитие искусственного интеллекта

происходило в своего рода нормативном вакууме (хотя и не абсолютном); за исключением действующих в некоторых государствах норм, касающихся беспилотных транспортных средств и летательных аппаратов, на настоящий момент принято весьма небольшое количество положений, которые касаются непосредственно уникальных специфических проблем, поднимаемых искусственным интеллектом. Практически отсутствует и судебная практика по данной тематике¹.

На данную сферу в любом случае распространяется действие законодательства, основной вопрос заключается лишь в том, достаточно ли действующих в настоящее время норм, которые устанавливают общий правовой режим, либо же таковые должны быть изменены с учетом особенностей искусственного интеллекта.

Исследование правового регулирования искусственного интеллекта и робототехники началось в 1970-х гг. в США. Там действовало более 100 университетских образовательных программ, включавших учебные курсы по искусственному интеллекту. Затем, в 1990-е гг., интерес к этой сфере распространился и на ряд других зарубежных стран. Тогда и были

приняты первые нормативные документы, регулирующие вопросы использования искусственного интеллекта. С 2015 г. проблематика искусственного интеллекта и робототехники стала признанной проблемой в большинстве стран мира и в интеграционных объединениях, выйдя на наднациональный уровень².

Сегодня многие государства мира задумались над вопросом урегулирования статуса и использования искусственного интеллекта.

В Республике Беларусь создание, обучение нейронных сетей и иных алгоритмов в специализированных разделах искусственного интеллекта, а также реализация результатов данной деятельности стимулируются посредством льготного правового и налогового режима, предоставленного Парку Высоких Технологий. Такая деятельность, согласно п. 3 Положения о Парке Высоких Технологий от 22 сентября 2005 г.³, дает основание к регистрации лица в качестве резидента Парка Высоких Технологий со всеми вытекающими преференциями. Формирование условий для развития искусственного интеллекта наряду с другими атрибутами цифровой экономики определено в Беларуси как одна из государственных задач. Вместе с тем

¹ Scherer M. U. Regulating artificial intelligence systems: risks, challenges, competencies, and strategies // *Harvard Journal of Law & Technology*. 2016. Vol. 29 (2). P. 356.

² Кашкин С. Ю. Искусственный интеллект и робототехника: возможность вторжения в права человека и правовое регулирование этих процессов в ЕС и мире // *Lex Russica*. 2019. № 7 (152). С. 155.

³ Положение о Парке высоких технологий: Декрет Президента Республики Беларусь от 22.09.2005 № 12: в ред. Декрета Президента Республики Беларусь от 21.12.2017 г. № 8 // Консультант Плюс: Беларусь [Электронный ресурс] / ООО «ЮрСпект», Нац. центр правовой информации Респ. Беларусь. Минск, 2020 (дата обращения: 27.04.2021).

правовое регулирование технологий искусственного интеллекта пока не вполне отвечает уровню современной науки и техники. Государственная программа развития цифровой экономики и информационного общества на 2016–2020 годы, утвержденная постановлением Совета Министров Республики Беларусь от 23 марта 2016 г. №235⁴, не содержит указаний ни на мероприятия по развитию искусственного интеллекта, ни на совершенствование правового регулирования в этой сфере. Законопроекты, регулирующие в той или иной мере рассматриваемые отношения, также пока не планируются. Не затрагиваются проблемы правового регулирования технологий искусственного интеллекта и в Декрете Президента Республики Беларусь от 21 декабря 2017 г. №8 «О развитии цифровой экономики»⁵.

Вместе с тем актуальность этих проблем нельзя недооценивать. Разработка методов и средств правового регулирования в сфере применения искусственного интеллекта включена в разряд приоритетных задач во многих государствах.

В законах и подзаконных актах целого ряда зарубежных государств уже сегодня закреплены обязанности государства содействовать развитию и контролю за разработкой, производством, распространением и использованием технологий и юнитов искусственного интеллекта.

Так, США, Япония, Китай, Южная Корея, Канада, Сингапур, и ряд других стран уже сегодня принимают регламентирующие меры в отношении робототехники и искусственного интеллекта.

Список литературы

1 Кашкин С. Ю. Искусственный интеллект и робототехника: возможность вторжения в права человека и правовое регулирование этих процессов в ЕС и мире // Lex Russica. 2019. № 7 (152). С. 151–159.

2 Scherer M. U. Regulating artificial intelligence systems: risks, challenges, competencies, and strategies // Harvard Journal of Law & Technology. 2016. Vol. 29 (2). P. 353–400.

⁴ О развитии цифровой экономики и информационного общества на 2016 – 2020 годы: Государственная программа, Постановление Совета Министров Республики Беларусь от 23.03.2016 № 235 // Консультант Плюс: Беларусь [Электронный ресурс] / ООО «ЮрСпект», Нац. центр правовой информации Респ. Беларусь. Минск, 2020 (дата обращения: 27.04.2021).

⁵ О развитии цифровой экономики: Декрет Президента Республики Беларусь от 21.12.2017 г. № 8 // Консультант Плюс: Беларусь [Электронный ресурс] / ООО «ЮрСпект», Нац. центр правовой информации Респ. Беларусь. Минск, 2020 (дата обращения: 27.04.2021).

Inga A. Sharapa

PhD (Law), Associate Professor,
Associate Professor of the Department of Civil Law Disciplines,
Belarusian State Economic University
(Minsk, Belarus)
inga1166000@gmail.com

**ANALYSIS OF EXISTING APPROACHES TO THE REGULATION OF
ARTIFICIAL INTELLIGENCE**

Abstract: The article conducts civil-legal research and understanding of the phenomenon of artificial intelligence, the state and features of its legal regulation, drawing public attention to the potential of artificial intelligence technology, the need to create a legal basis for the use of dynamic advances in information and communication technologies.

Keywords: artificial intelligence, robotics, intellectual property law.

Тарасова Людмила Валерьевна

Специалист по сопровождению образовательных программ,

Уральский федеральный университет

(г. Екатеринбург, Российская Федерация)

tlv.arb@yandex.ru

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КРИМИНАЛИСТИЧЕСКОМ ИССЛЕДОВАНИИ ПОДПИСЕЙ*

Аннотация: В статье рассматривается, как с развитием науки и техники изменялся подход к криминалистическому исследованию подписи. Автор делает краткий обзор истории внедрения компьютерных технологий в судебное почерковедение и почерковедческую экспертизу подписи, а также перспективе и проблемным вопросам использования ИИ для целей криминалистического исследования подписей.

Ключевые слова: подпись, криминалистические требования, экспертиза, искусственный интеллект (ИИ).

Для цитирования:

Тарасова Л. В. Проблемы использования искусственного интеллекта в криминалистическом исследовании подписей // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 116–121.

Судебное почерковедение находится в процессе постоянного поиска и применения более совершенных методов и средств криминалистического исследования подписей. Этот процесс связан с присущим для процесса оценки как отдельных, особенно частных признаков, так и всего комплекса идентификационных признаков, субъективизмом. Он связан с тем, что

«представление эксперта о ценности признака почерка всегда носит индивидуальный характер»¹. Подтверждением этого является обобщение экспертной практики по анализу первичных и повторных почерковедческих экспертиз, проведенное экспертом-криминалистом А. Н. Охлупиной, согласно которому обоснованием одних и тех же выводов разными

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16001 «Комплексное исследование правовых, криминалистических и этических аспектов, связанных с разработкой и функционированием систем искусственного интеллекта».

¹ Охлупина А. Н. Вопросы применения интеллектуальных систем в целях криминалистического исследования подписей // Энциклопедия судебной экспертизы: научно-практический журнал: сетевое электронное издание. 2016. № 1 (8). URL: http://www.proexpertizu.ru/theory_and_practice/pocherk/682 (дата обращения: 10.05.2021).

экспертами нередко служат различные совокупности признаков почерка, причём количество совпадений часто составляет не более двух признаков.

Помимо этого фактора следует указать и на особенности самой подписи как объекта почерковедческой экспертизы:

- малый объем графической информации,
- неинформативность (характерная для более чем 80 % современных русских подписей).

Развитие науки и техники, внедрение компьютерных технологий и систем искусственного интеллекта должно было стать гарантией полноты, объективности и всесторонности почерковедческой экспертизы, но на каждом этапе возникали проблемы, требующие решения. Современный этап не исключение.

Первый этап внедрения компьютерных технологий в исследовании подписей приходится на период с середины 70-х до середины 80-х гг. прошлого века, когда были разработаны и апробированы такие программы автоматизации количественного метода исследования подписи как «Мак» (Н. Г. Сахарова) и «APRIORI» (Ташкентский НИИСЭ). Данным средствам не удалось достичь широкого применения по многим причинам, среди них выделим следующие «технологические» причины:

- недостаточная надёжность созданных алгоритмов и их несоответствие требованиям экспертов-криминалистов и существующей практики,

- отсутствие достаточного количества оборудования,

- недостаточная мощность и технические характеристики оборудования.

С середины 80-х годов компьютеризация криминалистического исследования подписи направлена как на исследование почерковых объектов, так и на оформление результатов этих исследований. Для данного этапа следует отметить появление первой электронной системы изучения нажима по распределению плотности красителя в штрихах подписей, выполненных шариковой ручкой («Денситрон»), разработку полностью автоматических программ для исследования интегральных структурно-геометрических характеристик почерка («Телемак», позднее «ОКО» и «Маска») для определения подлинности подписей и появление метода фазового анализа письменных объектов («Diffaze», Э. Г. Хомяков). Самая известная и применяемая программа, «ОКО-1» (А. В. Смирнов, лаборатория СПЭ РФЦСЭ), позволяет определять априорную информативность подписи, плотность распределения красителя в штрихах подписи в разных режимах, возможность технической подделки подписи. Но и она не нашла достаточно широкого применения: на сегодняшний день так и не появилось процедуры, регламентирующей применение данных компьютерных технологий, и не сложилось единой судебной практики по отношению к выводам экспертов, ссылающихся в своих экспертных заключениях на данные,

полученные с помощью этих программ.

Несомненно, применение компьютерных технологий является перспективным направлением для решения задач криминалистического исследования подписей. И современный уровень развития науки и техники создаёт для развития этого направления все условия:

- появляются новые поколения компьютерной техники, качественно превосходящие своих предшественников,
- эта техника становится более доступной для экспертных, исследовательских и образовательных учреждений,
- получают развитие и широкое распространение системы ИИ, позволяющие перейти на качественно новый уровень проведения экспертиз благодаря возможности постоянно обучаться и принимать «разумные» решения.

Среди проблем, с которыми сталкивается процесс автоматизации работы эксперта-почерковеда, П. М. Кошманов выделил следующие:

- «современные системы ввода почерковой информации в компьютеры не позволяют в полной мере автоматизировать данный процесс,
- они не определяют многие свойства почерка»².

И решение этих проблем П. М. Кошманов видит в совершенствовании возможностей техники параллельно с научными разработками по созданию ИИ. Данную точку зрения мы полностью поддерживаем.

Отдельными экспертами-криминалистами предлагается ориентироваться ещё и на исследование динамических характеристик подписи с помощью ИИ, что ранее проводилось (наравне с исследованием статических характеристик) в биометрии, а в рамках судебно-почерковедческой экспертизы применялось только в отношении рукописных текстов³.

Следует отметить, что на сегодняшний день применение ИИ для криминалистического исследования подписей имеет больше теоретическо-исследовательский нежели практический характер, но разработки по прикладному использованию ИИ ведутся.

Для эффективного применения ИИ в целях криминалистического исследования подписей необходимо разработать:

1. стабильно работающие, корректно обучающиеся искусственные нейронные сети (системы ИИ), снабжённые системой защиты от несанкционированного доступа третьих лиц;
2. методические рекомендации и регламент по их применению.

² Кошманов П. М., Кошманов М. П. Этапы и основные направления внедрения компьютерных технологий в судебное почерковедение и почерковедческую // Эксперт-криминалист. 2008. № 3. С. 39.

³ Охлупина А.Н. Вопросы применения интеллектуальных систем в целях

криминалистического исследования подписей // Энциклопедия судебной экспертизы: научно-практический журнал: сетевое электронное издание. 2016. № 1 (8). URL: http://www.proexpertizu.ru/theory_and_practice/pocherk/682 (дата обращения: 10.05.2021).

По первому направлению разработчикам нейросетей необходимо решить множество вопросов:

- как гарантировать ввод достаточного и качественного обучающего «материала»,
- какие принципы и правила обучения внедрить в нейросеть,
- как контролировать правильность обучения нейросети поставленной задаче почерковедческого исследования,
- какие превентивные меры возможно применить, чтобы не допускать сбоев и ошибок,
- как научить нейросеть принимать экспертное решение по почерковедческим экспертизам и в каком виде его предоставлять,

- как обезопасить нейросеть от вмешательства извне.

По второму направлению самыми актуальными вопросами являются следующие:

- как распределить ответственность за принятое решение между экспертом и ИИ (или их разработчиками),
- какие методические рекомендации разработать,
- как гарантировать их соблюдение.

При корректном ответе на поставленные вопросы почерковедение сможет перейти на новый теоретический и практический уровень.

Список литературы

1. Бахтеев Д. В. Искусственный интеллект: этико-правовые основы: монография. М.: Проспект, 2021. 176 с.
2. Кошманов М. П. Использование компьютерных технологий в почерковедческой экспертизе (история и современное состояние) / М. П. Кошманов, П. М. Кошманов // Использование компьютерных технологий в экспертно-криминалистической деятельности: тезисы докладов науч.-практ. конф. Волгоград: ВЮИ МВД РФ, 1999. С. 63–66.
3. Кошманов М. П. О возможности объективизации оценки общих признаков почерка, отражающих структурные характеристики движений, с помощью компьютерных технологий / М. П. Кошманов, Р. И. Могутин, П. М. Кошманов // Использование компьютерных технологий в экспертно-криминалистической деятельности: тезисы докладов науч.-практ. конф. Волгоград: ВЮИ МВД РФ, 1999. С. 10–13.
4. Кошманов П. М. Повышение объективности почерковедческого исследования путем формализации оценки признаков / П. М. Кошманов, Р. И. Могутин // Криминалистика: актуальные вопросы теории и практики. Ростов-на-Дону: Ростовский ЮИ МВД России, 2002. С. 167–169.
5. Кошманов П. М. Этапы и основные направления внедрения компьютерных технологий в судебное почерковедение и почерковедческую экспертизу / П. М. Кошманов, М. П. Кошманов // Эксперт-криминалист. 2008. № 3. С. 35–40.

6. Ланцман Р. М. Кибернетизация почерковедческой экспертизы // Правоведение. 1966. № 4. С. 128–132.
7. Леканова Л. Г. О возможности применения количественных методов при исследовании кратких почерковых объектов / Л. Г. Леканова, А. В. Смирнов // Вопросы теории и практики судебной экспертизы. М., 1983. С. 47–53.
8. Леканова Л. Г. Определение вариационности и ее значение при решении задач экспертизы, связанной с исследованием малообъемных почерковых объектов / Л. Г. Леканова, Н. Г. Окромешко, В. Ф. Орлова // Экспертная техника: Актуальные вопросы судебно-почерковедческой экспертизы. 1981. Вып. 70. С. 3–49.
9. Леканова Л. Г. Типичные проблемные ситуации при исследовании малообъемных и кратких записей в судебно-почерковедческой // Экспертная техника: Актуальные вопросы судебно-почерковедческой экспертизы. 1981. Вып. 70. С. 70–84.
10. Ли Л. Е. Возможности совершенствования методики судебно-почерковедческой экспертизы подписей / Л. Е. Ли, В. Ф. Орлова, А. В. Смирнов // Использование специальных знаний на первоначальном этапе расследования: сб. науч. трудов. Волгоград: ВСШ МВД СССР, 1983. С. 50.
11. Ли Л. Е. Количественные методы и автоматизация в судебном почерковедении / Л. Е. Ли, А. В. Смирнов // Проблемы автоматизации, создания информационно-поисковых систем и применения математических методов в судебной экспертизе. М.: ВНИИСЭ, 1987. С. 47–53.
12. Липовский В. В. Экспериментальные данные о стереотипности некоторых структурно-геометрических характеристик подписей / В. В. Липовский, В. Н. Садиленко // Криминалистика и судебная экспертиза: сб. науч. работ. Киев, 1991. Вып. 42. С. 40–44.
13. Лобова О. С. Использование специальных компьютерных программ в почерковедческих исследованиях // Вестник Нижегородского Университета им. Н. И. Лобачевского: сер. Право, Уголовное судопроизводство в теории, зак-ве и конкретных жизненных ситуациях. 2006. Вып. 2 (10). С. 264–267.
14. Охлупина А. Н. Вопросы применения интеллектуальных систем в целях криминалистического исследования подписей // Энциклопедия судебной экспертизы: научно-практический журнал: сетевое электронное издание. 2016. № 1 (8). URL: http://www.proexpertizu.ru/theory_and_practice/pocherk/682.
15. Смирнов А. В. Программа «ОКО–1» для исследования кратких и простых почерковых объектов // Теория и практика судебной экспертизы: науч.-практ. журнал. 2006. № 1 (1). С. 121–124.

Liudmila V. Tarasova
Specialist in support of educational programs,
Ural Federal University
(Yekaterinburg, Russian Federation)
tlv.arb@yandex.ru

**TO THE ISSUE OF THE USE OF ARTIFICIAL INTELLIGENCE IN THE
FORENSIC EXAMINATION OF SIGNATURES***

Abstract: The article discusses an approach to forensic signature examination. The author gives a brief overview of the history of the introduction of computer technologies in forensic handwriting and handwriting examination of signatures, as well as future and problematic issues of using AI for the purposes of forensic examination of signatures.

Keywords: signature verification, forensic characteristics, examination, falsification, AI.

* The study was funded by RFBR according to the research project № 18-29-16001.

Салтыкова Алёна Евгеньевна

Студент,

Елецкий государственный университет им. И. А. Бунина

(г. Елец, Российская Федерация)

alena.saltykova16@gmail.com

Научный руководитель – Е. А. Очеретько, кандидат юридических наук, доцент
кафедры гражданского и предпринимательского права

ЮРИДИЧЕСКИЕ АСПЕКТЫ, СВЯЗАННЫЕ С ОБЩЕСТВЕННО ОПАСНЫМИ ПОСЛЕДСТВИЯМИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация: Широкомасштабное внедрение искусственного интеллекта во все сферы жизни становится одним из серьезных вызовов современного общества. В свою очередь, можно отметить отсутствие в законодательстве эффективных мер противодействия наступлению общественно опасных последствий в данной области. Отсутствует комплексный подход в разработке правовых норм, регулирующих применение технологий искусственного интеллекта, оценке рисков. Важным аспектом является необходимость выработки юридического определения искусственного интеллекта для формирования эффективной модели правового регулирования. В данной статье рассмотрены возможности использования искусственного интеллекта в юридической практике для решения ряда задач. Отмечается, что в настоящий момент существует много способов применения искусственного интеллекта, что несет в себе целый спектр рисков.

Ключевые слова: искусственный интеллект, правовое обеспечение искусственного интеллекта, юридическая ответственность, цифровая экономика, технологии.

Для цитирования:

Салтыкова А. Е. Юридические аспекты, связанные с общественно опасными последствиями применения искусственного интеллекта // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 122–127.

Искусственный интеллект – это способность интеллектуальных систем выполнять задачи, которые традиционно считаются прерогативой человека. История развития искусственного интеллекта в качестве самостоятельного научного

направления начинается в середине XX века. Однако еще до изобретения первых компьютеров специалистами разнообразных областей знания выдвигались идеи создания интеллектуальных машин, способных воссоздать процессы мышления

человека и в соответствии с этим перенять ряд задач.

Способности искусственного интеллекта по многим факторам оказались больше возможностей человека, даже с учетом достаточно узкого профиля их применения. В научной среде зародился вопрос: каковы границы возможностей компьютеров и достигнут ли машины уровня развития человека? Кроме того, разработка и распространение технологий искусственного интеллекта диктуют необходимость расширения механизмов правового регулирования данных процессов.

Правовая природа искусственного интеллекта, как и многих новаций цифрового общества, не является очевидной. В то же время влияние технологии распространяется практически на все сферы общественной жизни: медицину, экономику, образование, право. Ее применение неизбежно приводит к проблеме этического выбора, порождает правовые вопросы, требующие незамедлительного решения.

Как отмечают специалисты, единого ответа на вопрос, чем занимается искусственный интеллект, не существует. Последнее исследование Gartner о развитии искусственного интеллекта свидетельствует о большом разнообразии применений данной технологии на предприятиях. Эти программы способны воспринимать человеческую речь и производить вероятностный поиск, позволяют повышать продуктивность умственного труда человека, уменьшить объем рутинной работы.

Системы искусственного интеллекта применяются банками в страховой деятельности, а методы распознавания образов используют при распознавании текста и речи, в медицинской диагностике, а также для обеспечения ряда других задач национальной безопасности.

Искусственный интеллект, как автономный цифровой компьютер, способный к самообучению и интеллектуальным процессам, характерным для человека, существенно отличается от других явлений и объектов. В связи с этим, наиболее остро стоит вопрос об ответственности искусственного интеллекта за совершение общественно опасных деяний.

Первостепенным остается вопрос того, кто должен нести ответственность за действия интеллектуальных машин. Вследствие этого возникает потребность в формировании системы правовых мер противодействия преступлениям, совершаемым с применением искусственного интеллекта.

В современных российских реалиях нельзя сказать о нормативно-правовом регулировании возникновения, внедрения и применения технологий искусственного интеллекта как об эффективном процессе. Многие ученые и правоведы выдвигают предложения по принятию федерального закона, регулирующего правоотношения в сфере технологии искусственного интеллекта. Подобные предложения возникают по созданию специализированного федерального агентства по осуществлению контрольно-

надзорных функций в области робототехники и искусственного интеллекта¹.

Особенности использования и степень риска применения искусственного интеллекта, имеющие значение для правового регулирования, зависят от сферы его применения. Однако введение в оборот искусственного интеллекта при любых обстоятельствах сопровождается возникновением ряда проблем юридического характера. В настоящее время роботы не признаются в качестве субъекта права, их приравнивают к вещи, посредством которой могут быть созданы результаты интеллектуальной деятельности. Роботы не наделены правами и не несут юридическую ответственность. По общему принципу за все действия робота несет ответственность человек².

Актуальной в области применения искусственного интеллекта остается проблема безопасности, включающая не только защиту персональных данных, но и фактическую безопасность жизни и здоровья человека. Наглядно это показывает активное внедрение беспилотного транспорта. В 2018 году в США был зафиксирован первый в истории случай гибели человека под колесами беспилотного автомобиля. Трагедия произвела серьезный резонанс и повлияла на дальнейшую

разработку и тестирование беспилотных транспортных средств. На сегодняшний день нет единого мнения по вопросу юридической ответственности искусственного интеллекта за причиненный вред жизни и здоровью человека. В ряде случаев ставится вопрос о том, в каких сферах применение искусственного интеллекта в целом недопустимо или допустимо с соблюдением строгого контроля над его деятельностью, что противоречит сути функционирования искусственного интеллекта.

Таким образом, перспективной для законодателя в новых условиях становится задача обеспечения баланса между интересами общества, которые заключаются в использовании как можно большего потенциала новых технологий, и необходимостью минимизации негативных последствий использования инновационных технологий. Оценить реальные риски применения искусственного интеллекта в настоящий момент не представляется возможным, вследствие этого они приобретают непрогнозируемый характер.

В Европейском союзе рассматривается вопрос наделения искусственного интеллекта правосубъектностью, а также применения в отношении него термина «электронное лицо»³. Такой подход дает возможность определять

¹ Морхат П. М. К вопросу о специфике правового регулирования искусственного интеллекта и о некоторых правовых проблемах его применения в отдельных сферах // Закон и право. 2018. № 6. С. 63.

² Хисамова З. И., Бегишев И. Р. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты //

Всероссийский криминологический журнал. 2019. № 4. С. 564.

³ Кашкин С. Ю. Искусственный интеллект и робототехника: возможность вторжения в права человека и правовое регулирование этих процессов в ЕС и мире // Lex Russica. 2019. № 7. С. 151–159.

«электронное лицо» (будь то машина, робот, программа) как субъекта, обладающего способностью принимать осознанные и не основанные на заложенном создателем алгоритме решения и в силу этого наделенного совокупностью прав и обязанностей.

Ученые указывают на следующие признаки «разумности» роботов: умение анализировать данные; адаптировать свое поведение; наличие физической поддержки; приобретаемая посредством датчиков и контакта с окружающей средой автономия, способность к самообучению. Оценка степени сознания интеллектуальных машин создает возможность постановки вопроса о его правах и обязанностях. Следует отметить, что с учетом уровня развития и скорости обработки информации, превосходящей даже потенциальные возможности человека, искусственный интеллект остается программой с привязанным к ней материально-техническим обеспечением⁴.

Технологии искусственного интеллекта являются потенциально эффективно применяемыми в юридической практике. Искусственный интеллект позволяет обеспечивать корректное и быстрое решение различных задач для эффективного оказания юридических услуг.

В сфере юридической практики применение возможностей искусственного интеллекта может осуществляться в двух направлениях:

- моделирование юридических обоснований при помощи систем искусственного интеллекта, в том числе на основе прецедентного права (для чего нужно научить систему понимать определенные ключевые аспекты юридических рассуждений);
- создание вычислительных инструментов, основанных на искусственном интеллекте, используемых в рамках юридической практики или исследований (в целях поиска и выявления релевантных судебных решений, их сортировки согласно реализованным в них доктринальным подходам, выявления исторической значимости судебных решений).

Технологии искусственного интеллекта могут применяться в различных направлениях. Среди них перспективными являются: содействие в выработке решений по крупным объемам задач (как, например, в государственном и муниципальном управлении); обобщение и интеграция правовой информации, а также прогнозирование последствий принятия решений в отдельных сферах.

При помощи искусственного интеллекта можно производить предиктивный анализ судебной практики, направленный на прогнозирование. Правовая информация может включать фактические обстоятельства дела, прецеденты и исходы дел, поддающиеся машинному анализу.

⁴ Васильев А. А., Шпопер Д. Искусственный интеллект: правовые аспекты // Известия

Алтайского государственного университета. 2018. № 6. С. 23–26.

Таким образом, круг правовых проблем, которые возможно разрешить с использованием искусственного интеллекта, является весьма обширным, что говорит о многоаспектности применения данной технологии.

В заключение можно сделать вывод, что до принятия закона, регулирующего правоотношения в

сфере технологии искусственного интеллекта, остается правовая неопределенность в части возникновения, использования и распоряжения исключительными правами на результат интеллектуальной деятельности, созданный с помощью технологии искусственного интеллекта.

Список литературы

1. Васильев А. А. Искусственный интеллект: правовые аспекты / А. А. Васильев, Д. Шпопер // Известия Алтайского государственного университета. 2018. № 6. С. 23–26.
2. Кашкин С. Ю. Искусственный интеллект и робототехника: возможность вторжения в права человека и правовое регулирование этих процессов в ЕС и мире // Lex Russica. 2019. № 7. С. 151–159.
3. Морхат П. М. К вопросу о специфике правового регулирования искусственного интеллекта и о некоторых правовых проблемах его применения в отдельных сферах // Закон и право. 2018. № 6. С. 63–67.
4. Хисамова З. И. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты / З. И. Хисамова, И. Р. Бегишев // Всероссийский криминологический журнал. 2019. № 4. С. 564–574.

Alena E. Saltykova

Student,

Yelets State University named after I.A. Bunin

(Yelets, Russian Federation)

alena.saltykova16@gmail.com

Scientific supervisor – E. A. Ocheretko, PhD (Law), Associate Professor of the Department of Civil and Business Law

LEGAL ASPECTS RELATED TO PUBLIC HAZARDOUS EFFECTS OF THE USE OF ARTIFICIAL INTELLIGENCE

Abstract: Large-scale introduction of artificial intelligence in all spheres of life is becoming one of the serious challenges of modern society. In turn, there is the absence of effective measures in the legislation to counter the onset of socially dangerous consequences in this area. There is no comprehensive approach to the development of legal norms governing the use of artificial intelligence technologies, risk assessment. An important aspect is the need to develop a legal definition of artificial intelligence for the formation of an effective model of legal regulation. This article discusses the possibilities

of using artificial intelligence in legal practice to solve a number of problems. It is noted that at the moment there are many ways to use artificial intelligence, which carries a whole range of risks.

Keywords: artificial intelligence, legal support of artificial intelligence, legal responsibility, digital economy, technology.

Раздел III

РАСПРЕДЕЛЁННЫЙ РЕЕСТР, СМАРТ-КОНТРАКТЫ, КРИПТОВАЛЮТЫ И ИНЫЕ ЦИФРОВЫЕ ПРОДУКТЫ

УДК 343.34

Олифиренко Екатерина Павловна

Кандидат политических наук, доцент кафедры уголовно-правовых дисциплин,
Северо-Кавказская государственная академия
(г. Черкесск, Российская Федерация)

anna-54@bk.ru

ИСПОЛЬЗОВАНИЕ КРИПТОВАЛЮТЫ В ПРОТИВОПРАВНОЙ ДЕЯТЕЛЬНОСТИ: ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ

Аннотация: В статье рассматриваются отдельные аспекты использования виртуальной валюты при осуществлении противоправной деятельности. На основе анализа научной литературы, нормативных правовых актов, судебной практики выявлены актуальные проблемы в сфере контроля за оборотом криптовалют. Автором сформулированы основные направления противодействия преступлениям, совершаемым с помощью криптовалют.

Ключевые слова: цифровые финансовые активы, цифровая валюта, виртуальная валюта, платежная единица, криптовалюта, контроль, оборот, правоохранительная деятельность.

Для цитирования:

Олифиренко Е. П. Использование криптовалюты в противоправной деятельности: проблемы противодействия // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 129–137.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы¹ в качестве приоритетного направления внутренней политики определяет развитие информационных и коммуникационных технологий, формирование информационного пространства и соответствующей инфраструктуры. Однако применение цифровых технологий в современном мире способствовало активному развитию виртуальных

экономических отношений, в том числе и электронной коммерции, которая в настоящее время стала неотъемлемой и весьма значительной частью национальной экономики каждого государства. Вместе с развитием электронных платежных сервисов и цифровых технологий, а также использованием электронных и виртуальных валют, не только увеличилось количество преступных проявлений, но произошло и изменение преступности в целом, появились новые ее виды, а также

¹ О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента Российской

Федерации от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

новые предметы и средства совершения преступлений².

Появление инновационных способов совершения преступлений в сфере информационных технологий выявило проблему недостаточности принимаемых мер по противодействию этому виду современного криминала.

Предупреждение преступлений, совершаемых с использованием высоких технологий, является одним из приоритетных направлений деятельности органов внутренних дел³. Обеспечение своевременности и эффективности предупредительной деятельности в сфере информационно-телекоммуникационных технологий представляет собой первоочередную проблему для органов внутренних дел, решение которой во многом зависит от комплексного подхода к предупреждению данного вида преступлений.

Актуальной на сегодняшний день, на наш взгляд, является проблема противодействия

использованию криптовалют в противоправных целях и ответственности за совершение подобных деяний. Данной проблематике в последние годы посвящено много специальных работ⁴, но, тем не менее, остается ряд важных вопросов, требующих детальной проработки. В частности, одна из них, существующая в настоящее время нормативная неопределенность в регулировании криптовалютных операций, способствующая совершению преступлений с их использованием.

Следует отметить, что криптовалюта представляет собой реализацию перспективного направления для развития финансовой и экономической системы страны⁵, однако в российском законодательстве отсутствует понятие криптовалюты, как не определен и ее правовой статус.

В теории уголовного права дается несколько различных определений и понятий криптовалюты. Например, И. И.

² Пинкевич Т. В., Смольянинов Е. С. Международный опыт противодействия преступной деятельности с использованием криптовалюты: учебно-практическое пособие. Москва: Академия управления МВД России, 2021. 108 с.

³ Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. М.: Академия управления МВД России, 2019. Ч. 1. 208 с.

⁴ Долгиева М. М. Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалюты // Современное право. 2018. № 11. С. 103–108; Перов В. А. Выявление, квалификация и организация расследования

преступлений, совершаемых с использованием криптовалюты. М., 2017; Кучеров И. И. К вопросу о методике расследования преступлений, совершенных с использованием криптовалюты // Российский следователь. 2018. № 12. С. 17–21.

⁵ Вахрушев Д. С., Железов О. В. Криптовалюта как феномен современной информационной экономики: проблемы теоретического осмысления // Интернет-журнал Науковедение. 2014. № 5 (24). Режим доступа: Научная электронная библиотека «КиберЛенинка». URL: <https://cyberleninka.ru/article/n/kriptovalyuta-kak-fenomen-sovremennoy-informatsionnoy-ekonomiki-problemy-teoreticheskogo-osmysleniya> (дата обращения: 02.05.2021).

Кучеров определяет, что криптовалюты являются системным элементом современных альтернативных платежных систем⁶. А. И. Савельев относит криптовалюты к разновидностям электронного средства обмена⁷. В настоящее время криптовалюта находится в правовом вакууме. Так, сторонники использования криптовалют в России утверждают, что платежи и взаиморасчеты будут осуществляться быстрее, удобнее и безопаснее, однако данную позицию не разделяет руководство Центрального Банка России, поскольку, по его мнению, такие платежи будут способствовать увеличению числа фактов легализации (отмывания) доходов, полученных преступным путем.

С 2014 года в Российской Федерации предпринимались попытки запретить оборот криптовалюты. Так, в письме от 27 января 2014 года Банк России указал: «в связи с анонимным характером деятельности по выпуску «виртуальных валют» неограниченным кругом субъектов и по их использованию для совершения операций граждане и юридические лица могут быть, в том числе непреднамеренно, вовлечены в противоправную деятельность,

включая легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма» и предостерег граждан и финансовые организации от использования биткойн в качестве валюты или платежного средства⁸. В 2016 году Министерством финансов Российской Федерации был разработан законопроект, которым предлагалось ввести в Уголовный кодекс РФ статью, устанавливающую уголовную ответственность за оборот денежных суррогатов, к которым и была отнесена криптовалюта. Однако законопроект в данном виде не был внесен в Государственную Думу Российской Федерации.

Кроме того, Центральный банк России 4 сентября 2017 г. издал информационное письмо о высоких рисках при использовании и инвестировании в криптовалюты, подтвердив ранее высказанную позицию в отношении разного рода частных «виртуальных валют». В частности, Банк России указал, что большинство операций совершается вне правового регулирования⁹.

На данный момент можно предположить, что создание правовой базы, определяющий статус и оборот криптовалюты является вопросом времени¹⁰, поскольку судебная

⁶ Кучеров И. И. Криптовалюта как правовая категория // Финансовое право. 2018. № 5. С. 3–8.

⁷ Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование: 2-е издание. М.: Статут, 2016. С. 489–491.

⁸ Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн: информация Банка России от 27 января 2014 г. // СПС «Гарант». URL:

<https://www.garant.ru/products/ipo/prime/doc/70474620> (дата обращения: 03.05.2021).

⁹ Об использовании частных «виртуальных валют(криптовалют): информация Банка России от 04.09.2017. СПС «КонсультантПлюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_256266 (дата обращения: 03.05.2021).

¹⁰ Макаrchук Н. В. Публично-правовые ограничения как основание для определения

практика зачастую сталкивается с проблемами определения ущерба от хищения криптовалют либо с проблемами правильной квалификации содеянного. Говоря о нынешних тенденциях в судебной практике, следует отметить, что суды в целом перестают считать выпуск криптоактивов правонарушением и задумываются об их месте в системе объектов гражданских прав.

Так, в постановлении Седьмого арбитражного апелляционного суда от 16.07.2020 по делу № А45-28956/2019 говорится, что истец хотел включить в реестр требований к должнику обязательства по инвестиционному договору, где в качестве инвестиций передана виртуальная валюта Ethereum. Однако суд не признал Ethereum имуществом либо каким-либо денежным обязательством. Служители правосудия обратили внимание на опасность оборота таких средств, обусловленную возможной легализацией преступного дохода. Они сослались на письмо ЦБ РФ от 27.01.2014, которым наложено «табу» на оборот криптовалюты в качестве средств инвестиций и платежа. ЦБ стремится сохранить монополию рубля как платежного средства¹¹.

В условиях дефицита нормативного регулирования наивно

полагать, что наши судьи в лучших традициях прецедентного права смогут выработать сколько-нибудь удовлетворительное решение вопроса. Некоторые судьи пытаются осторожно включать в свои решения политико-правовые блоки, объясняя, почему они считают нужным ориентироваться на текущую политическую ситуацию, артикулируемую Президентом и Правительством. При отсутствии адекватного регулирования это представляется наилучшим выходом в сложившейся ситуации¹².

Отдельного обсуждения в рамках установления признаков конкретного состава преступления требует вопрос определения размера ущерба, причиняемого хищениями криптовалюты, поскольку, согласно отечественному законодательству, криптовалюта не имеет стоимости, однако фактически она имеет реальный курс и реальную цену и вопрос об ущербе от таких хищений несправедливо умалчивается¹³. Представляется логически верным, при определении суммы ущерба, причиненного хищением криптовалюты, исходить из сумм, реально затраченных на ее приобретение, по аналогии с хищением имущества.

криптовалют // Право и экономика. 2018. № 1. С. 22–25.

¹¹ Романенко Р. Н. Закон о цифровых финансовых активах // Юрист компании. Практический журнал для юристов. 2020. 21 дек. URL: <https://www.law.ru/article/23026-zakon-o-tsifrovyyh-finansovyh-aktivah> (дата обращения: 04.05.2021).

¹² Судебная практика по делам с использованием криптоактивов // Московские юристы – юридическая

консультация, суд: [сайт компании] URL: <https://kmcon.ru/articles/jurist/sudebnaya-praktika-po-delam-s-ispolzovaniem-kriptoaktivov.html> (дата обращения: 04.05.2021).

¹³ Долгиева М. М. Операции с криптовалютами: актуальные проблемы теории и практики применения уголовного законодательства // Актуальные проблемы российского права. 2019. № 4 (101). С. 128–139.

Уголовно-правовая доктрина в вопросах квалификации преступлений, совершаемых в сфере оборота криптовалюты, безусловно, связана с иными отраслями права, так, в частности, 31 июля 2020 года был опубликован Федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Данным законом регулируются отношения, связанные с выпуском и оборотом двух объектов – цифровых финансовых активов и цифровой валюты. В действующем законе проводится четкое разделение этих понятий. Так, статья 1 Федерального закон № 259 гласит, что под цифровыми финансовыми активами понимаются «цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном настоящим Федеральным законом, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в

информационную систему на основе распределенного реестра, а также в иные информационные системы»¹⁴.

Цифровой валютой признается совокупность электронных данных, содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации или иностранного государства, а также международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам¹⁵.

Вместе с тем принятый закон неоднозначно воспринят участниками криптосообщества, которые обнаружили ряд недостатков, в том числе «узких некорректных определений и терминов, а также слишком жестких, по их мнению, ограничений крипторынка»¹⁶.

¹⁴ О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 31.07.2020 № 259-ФЗ // СПС «КонсультантПлюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_358753/e21bf6629de12458b6382a7c2310cc359186da60 (дата обращения: 07.05.2021).

¹⁵ О цифровых финансовых активах, цифровой валюте и о внесении изменений в

отдельные законодательные акты Российской Федерации: федеральный закон от 31.07.2020 № 259-ФЗ // СПС «КонсультантПлюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_358753/e21bf6629de12458b6382a7c2310cc359186da60 (дата обращения: 07.05.2021).

¹⁶ Разбираем все минусы законопроекта о цифровых финансовых активах // BitJournal – Журнал о криптовалютной и финансовой сферах. URL: <https://bitjournal.media/01-02->

В феврале 2021 года к Федеральному закону №259-ФЗ «О цифровых финансовых активах...» были внесены дополнения, ужесточающие порядок регулирования, в первую очередь, оборота криптовалют. Изменения коснулись, в частности, статей Налогового кодекса, Кодекса об административных правонарушениях, Уголовного и Уголовно-процессуального кодексов, а также в Федеральном закона № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Так, изменения в Налоговом кодексе закрепляют статус имущества в отношении криптовалют, а также предусматривают обязанность физических и юридических лиц отчитываться перед налоговыми органами по всем операциям с криптовалютами в случае, если «сумма поступлений или списаний за календарный год превышает сумму, эквивалентную 600 т. р.»¹⁷.

Предлагаемыми поправками предусматривается также ряд штрафов, а неоднократный отказ от подачи налоговой декларации по операциям с криптовалютами в течение трех лет может привести и к уголовной ответственности. Систематическое нарушение требований закона может

наказываться штрафом, принудительными работами на срок до двух лет, либо арестом на срок до шести месяцев, при этом размер штрафа будет зависеть от размера суммы, в отношении которой не отчитывалось лицо.

Рассматриваемый законопроект устанавливает административную ответственность за незаконную организацию выпуска, незаконное совершение сделок с цифровыми финансовыми активами, а также за незаконный прием цифровой валюты в качестве встречного представления за товары, работы либо услуги. Незаконный оборот цифровых финансовых активов и нарушение правил совершения сделок будут наказываться максимальным штрафом до 2 миллионов рублей, а незаконный приём цифровой валюты в качестве оплаты за товары и услуги – максимальным штрафом до 1 миллиона рублей соответственно¹⁸.

Приобретение криптовалют в прежнем формате с 1 января 2021 года является законной операцией только для обычных граждан, отдельные категории граждан – к примеру, чиновники и сотрудники силовых структур уже не могут законно приобретать и продавать криптовалюты. В информационном письме Минтруда России № 18-2/10/В-12085 от 16 декабря 2020 года подробно изложены указанные

2018/razbiraem-vse-minusy-zakonoproekta-minfina-rf-o-tsifrovyyh-finansovyh-aktivah (дата обращения: 10.05.2018).

¹⁷ В Государственную Думу внесен законопроект о налоге на криптовалюту // Государственная Дума Федерального Собрания Российской Федерации: официальный сайт. Дата обновления:

01.12.2020. URL:

<http://duma.gov.ru/news/50155> (дата обращения: 07.05.2021).

¹⁸ Введут штрафы по КоАП за нарушения с цифровой валютой // Клерк.ру. Дата обновления: 11.11.2020. URL: <https://www.klerk.ru/buh/news/506898> (дата обращения: 04.05.2021).

ограничения. Так, с 1 января 2021 года чиновники, депутаты и иные специальные категории лиц, а также члены их семей не могут владеть цифровыми финансовыми активами, имеющими иностранное происхождение, а также цифровыми валютами, отнесенными к иностранным финансовым инструментам. До 1 апреля 2021 года указанные категории лиц обязаны избавиться от иностранных цифровых валют и цифровых финансовых активов¹⁹.

На февраль 2021 года перечисленные ограничения существуют только в виде законопроектов и в данный момент не имеют силы. Однако их активное лоббирование и запретительный характер наглядно иллюстрируют общее негативное отношение государственных органов к неконтролируемому, по их мнению, обороту цифровых валют. Подобный подход государственных структур к регулированию криптовалютных операций вызван не только опасениями относительно их бесконтрольного оборота, но и желанием заменить их в обороте на собственную цифровую валюту, выпускаемую непосредственно Центральным Банком. Так, в докладе Центрального банка Российской

Федерации сказано, что «цифровой рубль будет дополнительной формой российской национальной валюты и будет эмитироваться центральным Банком России в цифровой форме. Иными словами, цифровой рубль будет являться цифровой валютой российского центрального банка»²⁰.

Относительно интересной является тенденция к буквальному принуждению иностранных компаний работать только по российским правилам. Так, опубликованный 28 января 2021 года Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека первым же пунктом обязывает Администрацию Президента Российской Федерации совместно с Правительством Российской Федерации в срок до 1 августа 2021 года подготовить и представить предложения по установлению дополнительных требований к зарубежным технологическим компаниям, осуществляющим деятельность в российском сегменте информационно-телекоммуникационной сети Интернет, в том числе в части, касающейся открытия представительств этих компаний на территории Российской Федерации.²¹ На наш взгляд, такое правовое

¹⁹ О направлении информационного письма о возможности приобретения цифровых финансовых активов и цифровой валюты и владения ими отдельными категориями лиц: письмо Минтруда России от 16.12.2020 № 18-2/10/В-12085 // Законы, кодексы, нормативные и судебные акты. URL: <https://legalacts.ru/doc/pismo-mintruda-rossii-ot-16122020-n-18-210v-12085-o-napravlenii> (дата обращения: 04.05.2021).

²⁰ Цифровой рубль // Центральный банк РФ: официальный сайт. URL: <https://cbr.ru/StaticHtml/File/112957> (дата обращения: 10.05.2018).

²¹ Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека // Официальный сайт Президента РФ. URL: <http://www.kremlin.ru/acts/assignments/orders/64952> (дата обращения: 10.05.2018).

регулирование действительно несет в себе высокие риски для участников криптовалютного сообщества уйти в теневой сектор экономики, поскольку присутствием посредника в виде Центрального банка нарушается идея децентрализации.

Таким образом, нельзя отрицать очевидного факта внедрения криптовалют в жизнь современного общества, в связи, с чем государственные органы должны занять более лояльную позицию в отношении правового статуса криптовалюты. Принятие в Российской Федерации закона в сфере регулирования криптовалютных отношений, содержащего необходимые термины и понятия относительно криптовалютной деятельности и регламентирующего статус криптовалюты в России, позволит в дальнейшем разработать меры уголовно-правовой охраны объектов посягательств, которые в

настоящее время никак не регулируются.

Тот факт, что официальная статистика уголовных дел по преступлениям, совершаемых в сфере оборота криптовалюты, не фиксируется или выявляется сотрудниками правоохранительных органов в единичных случаях, говорит о высокой латентности указанного вида преступлений и об отсутствии профессиональной подготовки специалистов по их расследованию. В связи, с чем в Российской Федерации необходимо также разработать специальные правила и рекомендации по совершенствованию раскрытия и расследования преступных посягательств, связанных с нелегальным оборотом криптовалюты, используя опыт международного сотрудничества в сфере предупреждения цифровой преступности.

Список литературы

1. В Государственную Думу внесен законопроект о налоге на криптовалюту // Государственная Дума Федерального Собрания Российской Федерации: официальный сайт. Дата обновления: 01.12.2020. URL: <http://duma.gov.ru/news/50155>.
2. Вахрушев Д. С. Криптовалюта как феномен современной информационной экономики: проблемы теоретического осмысления / Д. С. Вахрушев, О. В. Железов // Интернет-журнал Науковедение. 2014. № 5 (24). Режим доступа: Научная электронная библиотека «КиберЛенинка». URL: <https://cyberleninka.ru/article/n/kriptovalyuta-kak-fenomensovremennoy-informatsionnoy-ekonomiki-problemy-teoreticheskogo-osmysleniya>.
3. Введут штрафы по КоАП за нарушения с цифровой валютой // Клерк.ру. Дата обновления: 11.11.2020. URL: <https://www.klerk.ru/buh/news/506898>.
4. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. М.: Академия управления МВД России, 2019. Ч. 1. 208 с.

5. Долгиева М. М. Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалюты // Современное право. 2018. № 11. С. 103–108.
6. Долгиева М. М. Операции с криптовалютами: актуальные проблемы теории и практики применения уголовного законодательства // Актуальные проблемы российского права. 2019. № 4 (101). С. 128–139.
7. Кучеров И. И. К вопросу о методике расследования преступлений, совершенных с использованием криптовалюты // Российский следователь. 2018. № 12. С. 17–21.
8. Кучеров И. И. Криптовалюта как правовая категория // Финансовое право. 2018. № 5. С. 3–8.
9. Макачук Н. В. Публично-правовые ограничения как основание для определения криптовалют // Право и экономика. 2018. № 1. С. 22–25.
10. Перов В. А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты. М., 2017.
11. Разбираем все минусы законопроекта о цифровых финансовых активах // BitJournal – Журнал о криптовалютной и финансовой сферах. URL: <https://bitjournal.media/01-02-2018/razbiraem-vse-minusy-zakonoproekta-minfina-rf-o-tsifrovyyh-finansovyh-aktivah>.
12. Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование: 2-е издание. М.: Статут, 2016.
13. Семеко Г. В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. 2020. № 1. С. 77–96.
14. Цифровой рубль // Центральный банк РФ: официальный сайт. URL: <https://cbr.ru/StaticHtml/File/112957>.

Ekaterina P. Olifirenko

Ph.D (Political Sciences), Associate Professor of Criminal law disciplines,
North-Caucasian State Academy
(Cherkessk, Russian Federation)
anna-54@bk.ru

THE USE OF CRYPTOCURRENCY IN ILLEGAL ACTIVITIES: PROBLEMS OF COUNTERACTION

Abstract: The article discusses some aspects of the use of virtual currency in the implementation of illegal activities. Based on the analysis of scientific literature, regulatory legal acts, and judicial practice, current problems in the field of control over the turnover of cryptocurrencies are identified. The author formulated the main directions of countering crimes committed with the help of cryptocurrency.

Keywords: digital financial assets, digital currency, virtual currency, payment unit, cryptocurrency, control, turnover, law enforcement.

Можаяева Людмила Евгеньевна

Старший преподаватель кафедры теории и истории государства и права,
Гомельский государственный университет имени Франциска Скорины
(г. Гомель, Республика Беларусь)
luda666@yandex.ru

Савченко Дмитрий Геннадьевич

Студент,
Гомельский государственный университет имени Франциска Скорины
(г. Гомель, Республика Беларусь)
savchenko_dmitryi@mail.ru

**КРИПТОВАЛЮТА В РЕСПУБЛИКЕ БЕЛАРУСЬ: ПРОБЛЕМЫ И ПУТИ
ИХ РЕШЕНИЯ**

Аннотация: В статье раскрываются вопросы использования технологии криптовалюты, особенности правового регулирования данной сферы. Автор предлагает понятие криптовалюты, анализирует возникающие проблемы правового, организационного и иного характера, а также предлагает направления их решения.

Ключевые слова: налогообложение, криптовалюта, Республика Беларусь, законодательство, регулирование.

Для цитирования:

Можаяева Л. Е. Криптовалюта в Республике Беларусь: проблемы и пути их решения / Л. Е. Можаяева, Д. Г. Савченко // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 138–142.

На данный момент мир вступил в стадию кардинальных высокоинтенсивных, динамических изменений и большинство сфер жизни современного человека переходят в IT-сферу, финансовые отношения не являются исключением. Миру давно известно о существовании пластиковых карт, системы бесконтактных платежей, совершивших своим появлением в 1950-х своеобразную технореволюцию.

Более 10 лет назад появилась, на наш взгляд, наиболее обсуждаемая и распространенная на данный момент криптовалюта – Bitcoin. Существует множество различных мнений насчет рациональности ее использования, стоимостных изменений, а также безопасности использования и государственного регулирования экономических отношений, связанных с использованием новых электронных систем платежей.

Считаем, что под криптовалютой следует понимать

децентрализованные виртуальные денежные единицы, не связанные с государственной валютной системой, эмитируемые в сети интернет и представляющие собой уникальный криптографический код.

В Республике Беларусь с 2017 года легализован оборот монет и токенов, то есть государство дало возможность приобретать, сбывать, обменивать и зарабатывать криптовалюту без уплаты какого-либо налога. Однако считаем необходимым отметить, что с 1 января 2023 года операции с криптовалютой будут являться предметом налогообложения¹.

На наш взгляд, жесткий контроль за криптовалютой, а также деятельностью, связанной с её использованием, со стороны государства необходим и позиция государства по вопросам налогообложения криптовалюты в ближайшие несколько лет является верной и обоснованной по ряду причин, которые будут упомянуты и раскрыты нами далее.

Проанализировав экономическую природу криптовалюты, можно заключить, что она, несомненно, является денежным суррогатом, зачастую фактически выступая в качестве средства платежа. Таким образом, вследствие отсутствия регламентации порядка ее использования защита прав граждан,

ставших жертвами мошенничества с криптовалютой, не представляется возможной.

Также считаем необходимым обратить внимание на тот факт, что «виртуальные валюты (криптовалюты) не имеют централизованного эмитента, единого центра контроля за транзакциями и характеризуются анонимностью платежей»². То есть фактически каждый отдельно взятый электронный кошелек конкретного пользователя является самостоятельным, неподконтрольным государству банковским учреждением, из этого следует высокая вероятность использования такой валюты в противоправных целях, например, при совершении коррупционных преступлений, финансировании террористической деятельности, легализации доходов, полученных преступным путем, преступлений, связанных с незаконным оборотом наркотиков и так далее.

Следует обратить внимание на волатильность криптовалюты. В частности, стоимость биткоина после достижения пика в 18949 долларов США на 17.12.2017 г., стала постепенно снижаться и уже 13.12.2018 составила всего 3352 долларов США, то есть упала практически в 6 раз, соответственно, как было нами упомянуто выше, никто из владельцев не был застрахован от

¹ Кому не продадут криптовалюту в Беларуси? // Myfin.by. Банки Беларуси. Кредиты. Вклады. Курсы валют. Дата обновления: 07.04.2021. URL: <https://myfin.by/stati/view/komu-ne-prodadut-kriptoalutu-v-belarusi> (дата обращения: 11.05.2021).

² Письмо Департамента налоговой и таможенной политики Минфина России от 2 октября 2017 г. № 03-11-11/63996 О регулировании выпуска и оборота криптовалют // ГАРАНТ – Законодательство. Garant.ru. Дата обновления: 05.12.2017. URL: <https://www.garant.ru/products/ipo/prime/doc/71714604/> (дата обращения: 11.05.2021).

такого падения курса, их права не были защищены со стороны государства. Не исключено, что после текущего очередного рекордного, стремительного подъема стоимости Bitcoin, в отсутствие обеспеченности данной валюты, например, золотом, она столь же стремительно упадёт и, если не обесценится, то значительно, в десятки раз потеряет свою нынешнюю стоимость³.

Также на такую валюту легко оказать влияние в интересах каких-либо конкретных лиц либо групп населения, примером может служить события июля 2016 года, когда у пользователей криптовалюты Ethereum (аналога Bitcoin) исчезли из обращения в общей сложности около 50 млн. долларов США. Деньги неожиданно оказывались на счету у одного из участников проекта, который не мог на них правомерно претендовать, но при этом условий контракта он не нарушал.

Если бы это произошло в реальном мире, пользователи могли бы обратиться в суд либо оспорить условия контракта, связаться с банком и попросить заблокировать счет. Но данные события происходили в интернете, вложенные деньги исчислялись не в долларах, а в единицах распределенной криптовалюты Ethereum. Особенным являлось и то, что действия по электронному контракту совершали компьютеры. Поэтому его практически невозможно было

нарушить, отменить или обойти, а если его участник хотел выйти из организации, то для возврата вложенных денег создавалась дочерняя организация, куда переводились средства из основной.

Как выяснилось позже, в результате ошибки в машинном коде эту операцию можно повторять бесчисленное множество раз, чем и воспользовался злоумышленник. За короткое время он перевел в свою дочернюю организацию сумму, равную примерно 50 миллионам долларов США. Причем эти деньги вернуть обратно мог только сам злоумышленник, но этого делать он не собирался, поскольку формально не нарушил условий контракта⁴.

По нашему мнению, так как добыча криптовалюты осуществляется как посредством майнинга, для которого необходимы значительные мощности вычислительных машин, компьютеров, так и посредством простого приобретения, то физическое лицо фактически вкладывает свои денежные средства с перспективой того, что курс криптовалюты, в которую он вложился, вырастет. Это похоже на популярные в девяностых, также имеющие место и в современном мире, «инвестиции под высокий процент», то есть финансовые пирамиды, которые в итоге прекращали своё существование, а обманутые инвесторы оставались ни с чем, только

³ РБК Кripto // Rbc.ru. Дата обновления: 11.05.2021. URL: <https://www.rbc.ru/crypto/currency/btcusd> (дата обращения: 11.05.2021).

⁴ Степанов О. А., Печегин Д. А. Защита национальной экономики: современные проблемы правового регулирования // Право. Журнал Высшей школы экономики. 2017. № 4. С. 83–96.

в современном информационном обществе «билеты» стали заменяться блокчейнами и криптошифрами, то есть имеет место изменение формы, но не фактического содержания.

На данный момент правительства многих стран мира озадачены ситуацией с криптовалютой и вырабатывают меры по регулированию отношений, с ней связанных. Так, например, в Южной Корее: «власти рассматривают возможность введения налога в 20 процентов, аналогично сбору, уплачиваемому от выигрыша в лотерею, доходы от инвестиций в криптовалюту в Японии облагаются вплоть до 55 процентов, во Франции – 25 процентов»⁵.

Таким образом:

1. Законодательство

Республики Беларусь, касательно операций с криптовалютой, – одно из самых передовых в современном мире.

2. Операции с криптовалютой на территории Республики Беларусь

на данный момент являются законными.

3. Для покупки криптовалюты в Республике Беларусь необходимо пройти верификацию личности, также не удастся приобрести криптовалюту резидентам из запрещенных юрисдикций.

4. При использовании криптовалюты, приобретенной на неофициальных платформах, лицо, ее использующее, в должной мере не является защищенным со стороны государства, в случае ее утраты, падения стоимости.

5. Ввиду вышеупомянутой возможности использования криптовалюты в преступной деятельности, считаем целесообразным наделить исключительным и всеобъемлющим правом контроля за всеми операциями с криптовалютой Департамент финансового мониторинга Комитета государственного контроля Республики Беларусь.

Список литературы

1. Кому не продадут криптовалюту в Беларуси? // Myfin.by. Банки Беларуси. Кредиты. Вклады. Курсы валют. Дата обновления: 07.04.2021. URL: <https://myfin.by/stati/view/komu-ne-prodadut-kriptovalutu-v-belarusi>.

2. Налогообложение криптовалют в мире // Криптовалюта. Tech – Cryptocurrency.tech. Дата обновления: 12.02.2020. URL: <https://cryptocurrency.tech/nalogooblozhenie-kriptoalyut-v-mire-gde-kak-i-glavnoe-skolko/>.

3. Степанов О. А. Защита национальной экономики: современные проблемы правового регулирования / О. А. Степанов, Д. А. Печегин // Право. Журнал Высшей школы экономики. 2017. № 4. С. 83–96.

⁵ Налогообложение криптовалют в мире // Криптовалюта. Tech – Cryptocurrency.tech. Дата обновления: 12.02.2020. URL:

<https://cryptocurrency.tech/nalogooblozhenie-kriptoalyut-v-mire-gde-kak-i-glavnoe-skolko/> (дата обращения: 11.05.2021).

Lyudmila E. Mozhayeva

Senior Lecturer at the Department of Theory and History of State and Law,
Francisk Skorina Gomel State University
(Gomel, Republic of Belarus)
luda666@yandex.ru

Dmitryi H. Savchenko

Student,
Francisk Skorina Gomel State University
(Gomel, Republic of Belarus)
savchenko_dmitryi@mail.ru

TAXATION OF CRYPTOCURRENCY IN THE REPUBLIC OF BELARUS

Abstract: The article reveals the issues of using cryptocurrency technology, features of the legal regulation of this area. The author proposes the concept of cryptocurrency, analyzes the emerging problems of a legal, organizational and other nature, and also proposes directions for their solution.

Keywords: taxation, cryptocurrency, The Republic of Belarus, legislation, regulation.

УДК 343.97

Ржанникова Светлана Сергеевна

Старший преподаватель кафедры криминалистики,
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
ssr80@mail.ru

Лобанов Руслан Эльмирович

Командир отделения 2 курса, курсант,
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
ruslanwww@inbox.ru

НЕКОТОРЫЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБОРОТА КРИПТОВАЛЮТЫ

Аннотация: В статье рассмотрены некоторые особенности оборота криптовалюты, ее статус в правоотношениях на современном этапе, а также использование цифровой валюты при совершении преступлений. Проанализировано правовое регулирование оборота криптовалюты, выявлены проблемные аспекты, внесены предложения по совершенствованию законодательной регламентации использования криптовалюты в общественных отношениях.

Ключевые слова: криптовалюта, биткоин, блокчейн, майнинг, цифровая валюта, денежная единица.

Для цитирования:

Ржанникова С. С. Некоторые аспекты правового регулирования оборота криптовалюты / С. С. Ржанникова, Р. Э. Лобанов // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 143–147.

Более 12 лет назад в обороте появилась первая криптовалюта – Биткоин, на сегодняшний день зарегистрировано больше тысячи различных видов криптовалют. В настоящее время институт цифровой валюты набирает все большую популярность, но законодательство в этой сфере не в полном объеме закрепляет все возможные правоотношения.

В Российской Федерации криптовалюта не признана как валюта, поскольку, согласно статье 27 федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации», официальной денежной единицей (валютой) Российской Федерации

является рубль¹. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» дает определение цифровой валюте, закрепляет процесс регистрации цифровых финансовых активов и ответственность операторов выпускаемых цифровые активы².

Система «биткоин» стала началом технологии «блокчейн». Блокчейн – это один из вариантов реализации сети распределенных реестров, база данных с четкой структурой и своими правилами, в которой структурируются данные о совершенных транзакциях в виде цепочки последовательно связанных блоков транзакций³. Технология блокчейн является основой для большинства популярных криптовалют, которых в настоящее время насчитывается около тысячи видов. Преимущество технологии – исключение возможности кражи или мошенничества. Это своеобразная тетрадь, где отображена вся информация о переводах виртуальной валюты.

Майнинг – это процесс добычи криптовалюты. Для этой добычи

используется ресурс компьютера (процессор, видеокарта). Криптоджекинг – это использование ресурса стороннего персонального компьютера, с целью добывания криптовалюты. То есть, злоумышленник создает вредоносный код, который запускает программу для майнинга и добывает со стороннего компьютера криптовалюту, не ставя в известность владельца компьютера. Все эти отношения возникли совершенно недавно, с появлением криптовалюты.

На различных теневых ресурсах «Darknet», при помощи криптовалюты производится продажа наркотических средств, оружия, заказываются всевозможные незаконные услуги, как, например, взлом личных страниц в социальных сетях, предоставление личной информации или переписки.

Благодаря анонимности цифровой валюты, злоумышленники совершают различные преступления. Некоторые компании уклоняются от уплаты налогов путем совершения сделок за криптовалюту.

Данное явление правоохранительным органам очень сложно отследить, поскольку все кошельки, как и сама валюта, анонимны. Но, в тоже время, при

¹ О Центральном банке Российской Федерации: федеральный закон от 10.07.2002 № 86-ФЗ // Официальный интернет-портал правовой информации pravo.gov.ru. URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102077052> (дата обращения: 10.05.2021).

² О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 31.07.2020 № 259-ФЗ // Официальный

интернет-портал правовой информации pravo.gov.ru. URL: <http://publication.pravo.gov.ru/Document/View/0001202007310056> (дата обращения: 10.05.2021).

³ Обзор по криптовалютам, ICO (initial coin offering) и подходам к их регулированию / Центральный банк Российской Федерации // Официальный сайт Центрального Банка РФ. 2017. дек. С. 3. URL: https://cbr.ru/content/document/file/36009/rev_ico.pdf (дата обращения: 10.05.2021).

совершении сделок, в общем реестре сервисов крипто-кошельков, содержится информация об участниках сделки. Если иметь доступ к этому реестру, то можно отследить, кто, когда и сколько перевел криптовалюты, но на данный момент, такой возможности нет.

Так, в январе 2020 г. Шамионова Ю. В., совершая преступление в сфере незаконного оборота наркотических средств на территории Пензенской области, имея преступный умысел на придание правомерного вида владению, пользованию и распоряжению денежными средствами, полученными от незаконного сбыта наркотических средств, воспользовалась преступной схемой, согласно которой, денежные средства, полученные ею за выполненную работу по оборудованию тайников (закладок) с наркотическими средствами, поступали путем совершения финансовых операций в виде криптовалюты bitcoin, с обезличенных bitcoin-кошельков, на находящиеся в ее пользовании, одноразовые обезличенные bitcoin-кошельки. Впоследствии с учетом курса Российского рубля с вышеуказанного сайта Шамионова Ю.В. получала денежные переводы с лицевых счетов, оформленных в системе Visa QIWI Wallet ЗАО «Киви Банк», в том числе с лицевых счетов лиц, неосведомленных о преступном происхождении переводимых денежных средств, на свои лицевые счета⁴.

Согласно общим правилам, криптовалюта не является имуществом, в законе используется термин «цифровая валюта» – совокупность электронных данных (цифрового кода или обозначения). В соответствии с законодательством, не допускается принимать цифровую валюту в качестве средства платежа в счет оплаты, однако, оплачивать что-либо криптовалютой напрямую не запрещено.

На основании новых правил, владельцы цифровой валюты обязаны ее декларировать, только при таком условии можно будет требовать в суде нарушенных прав, связанных с криптовалютой. Однако, некоторые категории граждан все-таки обязаны декларировать наличие криптовалюты независимо от желания обращаться за защитой своих интересов в суд – это государственные служащие, сотрудники государственных корпораций.

На сегодняшний день в Налоговом кодексе не предусмотрены особенности расчета и уплаты налогов с доходов, полученных при использовании криптовалюты. В декабре 2020 года в Государственную думу внесен законопроект, который предусматривает ответственность за отсутствие отчета об операциях и остатках на счетах цифровой валюты, а также за неуплату налогов с криптовалютных операций. Предлагается ввести штраф в размере 40 % от неуплаченной суммы доходов при использовании криптовалюты и 10 % от имеющейся суммы

⁴ Приговор Железнодорожного суда г. Пензы № 1-117/2020 от 13 июля 2020 г. по делу № 1-117/2020 // СудАкт. URL:

<https://sudact.ru/regular/doc/UiZXB0FNFyNc/> (дата обращения: 10.05.2021).

криптовалюты при непредоставлении сведений об ее наличии⁵.

В свою очередь, Министерство финансов России совершенно справедливо предложило внести изменения в Уголовный кодекс РФ за непредоставление деклараций о владении криптовалютой и операций с ней.

Несмотря на делающиеся шаги в сторону урегулирования оборота криптовалюты и введения ответственности за ее незаконное использование, в современном законодательстве недостаточно полно предусмотрены правоотношения с цифровой валютой и зачастую

злоумышленники могут остаться безнаказанными. На наш взгляд, необходимо ужесточить правоотношения в данной отрасли. Поэтому, мы считаем целесообразным также внести дополнительную норму в статью 159 УК РФ «Мошенничество», предусмотрев факт завладения криптовалютой незаконным путем.

В свою очередь, в целях предупреждения преступлений в информационной сфере необходимо повысить уровень информационной грамотности населения, включив в школьный курс информатики темы по кибербезопасности.

Список литературы

1. Обзор по криптовалютам, ICO (initial coin offering) и подходам к их регулированию / Центральный банк Российской Федерации // Официальный сайт Центрального Банка РФ. 2017. дек. С. 3. URL: https://cbr.ru/content/document/file/36009/rev_ico.pdf.

Svetlana S. Rzhannikova

Senior Lecturer of the Department of Criminalistics,
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
ssr80@mail.ru

Ruslan E. Lobanov

Cadet,
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
ruslanwww@inbox.ru

SOME ASPECTS OF LEGAL REGULATION OF CRYPTOCURRENCY TURNOVER

⁵ Законопроект № 1065710-7 «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации

(в части налогообложения цифровой валюты)» // <https://sozd.duma.gov.ru> (Дата обращения 12.05.2021 г.)

Abstract: The article discusses some features of the turnover of cryptocurrency, its status in legal relations at the present stage, as well as the use of digital currency in the commission of crimes. The legal regulation of cryptocurrency turnover is analyzed, problematic aspects are identified, and proposals are made to improve the legislative regulation of the use of cryptocurrency in public relations.

Keywords: cryptocurrency, bitcoin, blockchain, mining, digital currency, monetary unit.

Гридасов Владислав Денисович

Студент,

Уральский государственный юридический университет

(г. Екатеринбург, Российская Федерация)

slawa.gridasov@yandex.ru

Научный руководитель – Е. В. Дженакова, старший преподаватель кафедры
информационного права

ИЗМЕНЕНИЕ ПРАВОВОГО РЕЖИМА КРИПТОВАЛЮТЫ В РОССИИ НА ОСНОВЕ ЗАРУБЕЖНОГО ОПЫТА

Аннотация: В 2009 году появилась новая технология – криптовалюта. Вследствие её специфических особенностей многие страны по-разному подходят к правовому регулированию криптовалюты. До сих пор не определен ее общий международно-правовой режим, не установлены единые международные стандарты и правила, позволяющие унифицировать механизм правового регулирования криптовалюты. Эта проблема приводит к ограничению оборота криптовалюты и её развития. В данной статье рассматриваются существующие в современном мире различные механизмы (модели) правового регулирования виртуальных валют. На основе их анализа предлагается один из вариантов изменения правового режима криптовалюты в России.

Ключевые слова: криптовалюта, цифровые финансовые активы, модели правового регулирования, виртуальная валюта, оборот.

Для цитирования:

Гридасов В. Д. Изменение правового режима криптовалюты в России на основе зарубежного опыта // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 148–156.

В современном мире вопрос правового регулирования криптовалюты является крайне актуальным. Исходя из ее специфических признаков сложно прийти к общему международно-правовому режиму и многие страны по-разному подходят к данному вопросу. Россия с июля 2020 года приняла Федеральный закон «О цифровых финансовых активах», тем самым ввела определенный правовой

режим криптовалюты. Однако до сих пор деятельность по обороту виртуальных валют в России не пользуется спросом, так как правовое регулирование данной деятельности противоречит их сущности. Под криптовалютой понимается автономное децентрализованное платежное средство, используемое для осуществления денежных расчетов в информационном экономическом пространстве на основе блокчейна,

технологиях распределенного реестра и на криптографических методах, гарантирующих анонимность ее владельцам¹.

В национальном законодательстве зарубежных стран следует выделить три существующие модели правового регулирования оборота криптовалют: запрещающая, ограничивающая и позволяющая².

К первой модели относятся страны, полностью запретившие оборот криптовалюты и признавшие её рискованным финансовым инструментом. Законодательство данных стран объясняет это потенциальным вредом для национальных финансовых систем. К таким странам относятся Боливия, Египет, Непал, ОАЭ, Саудовская Аравия и т. д. Например, в Египте использование криптовалюты считается харамным, то есть греховным деянием с точки зрения ислама, в Непале криптовалюту запретили полностью в любом виде, в Боливии она запрещена с 2014 года, а финансовые операции, занимающиеся её оборотом, объявлены вне закона и названы финансовыми пирамидами, о чём постоянно напоминают гражданам³.

Однако можно заметить постепенный отход от полного запрета использования криптовалюты. Например, несмотря на запрет в ОАЭ с 2017 года на транзакции с

виртуальной валютой, уже в 2018 году была выдана лицензия на совершение торговых операций с криптовалютой без права конвертации её в фиатные деньги. В начале того же года о сотрудничестве с целью создания собственной криптовалюты заявили в Саудовской Аравии. Также в Египте власти решили пересмотреть свою позицию из-за более тесной вовлеченности соседних стран в сферу цифровых денег. Исходя из этого можно сделать вывод о неперспективности *запретительной* модели, так как она значительно сокращает технологический прогресс и снижает уровень инвестиционной привлекательности.

Специфика второй модели правового регулирования криптовалюты заключается в стремлении государств защитить свои национальные финансовые системы от потенциальной угрозы со стороны автономно существующих криптовалют при сохранении необходимых правовых основ для использования технологии распределённых реестров. *Ограничения* в данных странах носят различный характер, рассмотрим три наиболее популярные формы ограничения.

Особенность правового регулирования криптовалюты в Бахрейне, Катаре, Кувейте и Омане заключается в *запрете использования*

¹ Глобенко О. А., Ильягуева А. А. Криптовалюта: проблемы правового регулирования и доктринального определения // Образование и право. 2018. № 3. С. 135–140.

² Аманжолова Б. А. Правовое регулирование криптовалют в мире // Образование и право. 2018. № 5. С. 228–231.

³ В каких странах запрещено использовать Биткойн // Портал finswin.com. URL: <https://finswin.com/kripto/btc/gde-zapreshchen-bitkoin.html> (дата обращения: 15.05.2021).

криптовалюты финансовым организациям, но центральные банки данных стран выразили намерение по созданию цифровых валют, обеспеченных в свою очередь национальной валютой, вследствие чего будут признаны законным платёжным средством⁴.

В азиатских странах ограничение носит несколько иной характер. В 2018 году в Китае Народный Банк Китая, Комиссия по банковскому регулированию, Министерство общественной безопасности и Государственная администрация по рыночному регулированию выступили с совместным заявлением, в котором указывалось, что «монеты и киберденьги, которые называются криптовалютой» не являются законным платёжным средством и не подлежат обязательному приему в качестве встречного исполнения по обязательствам, а также не могут быть эмитированы официально уполномоченными на выпуск денежных средств на территории КНР субъектами⁵. Это означает, что криптовалюта не имеет статуса национальной валюты. В апреле 2019 года Национальная комиссия по

реформам развития Китая включила деятельность по созданию новых единиц криптовалюты («майнинг») в список видов деятельности, которые подлежат запрету в связи с их вредоносным характером для национальной экономики и окружающей среды⁶. Но, несмотря на данные нормативные правовые акты, на территории КНР остаётся правомочие владения, носящее исключительно вещный характер и не позволяющее реальное использование виртуальных валют в имущественном обороте.

Особенность правового регулирования криптовалюты в некоторых странах Европы проявляется в частичном регулировании некоторых видов деятельности с криптовалютой. В 2014 году Банк Литвы выпустил предостережение, согласно которому виртуальные валюты не являются законным средством платежа, а их использование носит заведомо рискованный характер⁷. Затем Банк сделал заявление, согласно которому предоставление финансовых услуг не может быть сопряжено с использованием виртуальных валют⁸. Это означает, что запрещается

⁴ Информация пресс-службы ЦБ РФ «Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн» // Центральный Банк РФ: официальный сайт. URL: <http://www.cbr.ru/press/PR/> (дата обращения: 15.05.2021).

⁵ Notice adopted by the People's Bank of the PRC // The People's Bank of the PRC: official site. URL: http://www.pbc.gov.cn/publish/goutongjiaoiu/524/2013/20131205153156832222251/20131205153156832222251_.html (accessed: 15.05.2021).

⁶ Chan E. China Plans to Ban Cryptocurrency Mining in Renewed Clampdown // Bloomberg. URL: <https://www.bloomberg.com/news/articles/2019-04-09/china-plans-to-ban-cryptocurrency-mining-in-renewed-clampdown> (accessed: 15.05.2021).

⁷ Čiulada P. Lietuvos bankas apsisprendė dėl bitkoinų // Verslo žinios. URL: <https://www.vz.lt/archive/article/2014/1/31/lietuvos-bankas-perspeja-del-bitkoinu> (accessed: 15.05.2021).

⁸ Press Release. Bank of Lithuania. Bank of Lithuania Announces Its Position on Virtual Currencies and ICO (Oct. 11, 2017) // Bank of

продажа криптовалюты, создание технических условий для использования криптовалюты при проведении расчетов, а также осуществление операций по обмену криптовалюты на реальные деньги. Однако осуществляется регулирование деятельности специальными нормативными правовыми актами в зависимости от цели размещения криптовалюты: привлечение инвестиций, оказание услуг по инвестиционной деятельности, краудфандинг и т. п., что фактически рассредоточивает правовые нормы по нескольким источникам и не предполагает принятия единого правового акта.

Большая часть стран Европы и Северной Америки прибегают к *дозволительной модели* правового регулирования криптовалюты. Её суть в стремлении не устанавливать законодательных ограничений на использование криптовалюты в имущественном обороте, сдерживая при этом ее платежеспособность в целях поддержания устойчивости национальных платежных систем.

Национальная позиция Великобритании об использовании криптовалюты отражена в поправках к «Четвертой Директиве о противодействии отмыванию доходов», которые вступили в силу в начале 2020⁹. В соответствии с данными поправками вводится законодательное определение понятия

«виртуальных валют»: цифровое представление стоимости, которое не выпущено и не гарантировано центральным банком или органом государственной власти, но при этом принимается физическими и юридическими лицами как средство обмена, которое хранится и передается в электронном виде. Особенностью данного определения является отсутствие указания на использование технологий криптографического шифрования, что позволяет использовать термин «виртуальные валюты» как в отношении криптовалюты, основанной на блокчейне, так и в отношении иных видов виртуальных валют¹⁰. Данный подход представляется весьма перспективным, поскольку обеспечивает безопасность посредством контроля государства за обменом криптовалюты.

Одну из прогрессивных позиций в отношении *дозволительной модели* занимает Япония: в 2017 году были приняты соответствующие поправки к «Национальному Закону о платежных сервисах». В новой редакции данного акта было отражено нормативное определение «виртуальной валюты» – имущественная ценность, что подчеркивает имущественный характер, а также требование по обязательной регистрации лиц, осуществляющих деятельность по обмену виртуальной валюты на

Lithuania: official site. URL: <https://www.lb.lt/en/news/bank-of-lithuania-announces-its-position-on-virtual-currencies-and-ico> (accessed: 15.05.2021).

⁹ Dewey J. Global Legal Insights: Blockchain & Cryptocurrency Regulation // The Association of Corporate Counsel. URL:

https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf (accessed: 15.05.2021).

¹⁰ Середа А. В., Ручкина Г. Ф. Зарубежный опыт правового регулирования оборота виртуальных валют: модели и подходы // Образование и право. 2019. № 7. С. 99–103.

фиатные деньги¹¹. Осуществление данной деятельности без получения соответствующей лицензии квалифицируется как преступление. Дальнейшее совершенствование национального законодательства Японии привело к принятию нового пакета поправок, вступившего в силу в апреле 2020: требование по обязательному лицензированию распространяется на лиц, осуществляющих хранение криптовалюты, даже если такие субъекты правоотношений не осуществляют операций по ее обмену. Также были установлены лимиты по максимально допустимым маржинальным сделкам с криптовалютой. Таким образом, можно сделать вывод, что основной задачей японского правительства является обеспечение безопасного и правомерного функционирования большого количества криптовалютных бирж, зарегистрированных в стране и осуществляющих операции с большим объемом цифровых активов.

Обратимся к российскому законодательству для определения правового регулирования криптовалюты, а именно к Федеральному закону «О цифровых финансовых активах» от 31.07.2020, который вступил в силу 01.01.2021 года¹².

Прежде всего закон определяет правовое положение криптовалюты:

согласно п. 2 и п. 3 ст. 1 ФЗ «О цифровых финансовых активах» цифровые финансовые активы являются *имуществом* и могут быть приняты в качестве *средства платежа и инвестиций*; цифровые финансовые активы *не являются денежной единицей на территории РФ*.

Важным моментом в ФЗ «О цифровых финансовых активах» становится определение условий выпуска цифровых финансовых активов, определение субъектов, которые могут заниматься данной деятельностью, а также установление правил обмена криптовалюты. Права, удостоверенные цифровыми финансовыми активами, возникают у их первого обладателя с момента его внесения в информационную систему, в которой осуществляется выпуск цифровых финансовых активов. В качестве номинального держателя цифровых финансовых активов может выступать только лицо, *имеющее лицензию* на осуществление депозитарной деятельности.

Основными участниками оборота цифровых финансовых активов являются лицо, имеющее лицензию, и оператор информационной системы¹³. Оператор информационной системы – ключевое звено в обороте криптовалюты в России, так как только через него лица способны обмениваться цифровыми

¹¹ Dewey J. Global Legal Insights: Blockchain & Cryptocurrency Regulation // The Association of Corporate Counsel. URL: https://www.acc.com/sites/default/files/resources/v1/membersonly/Article/1489775_1.pdf (accessed: 15.05.2021).

¹² СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 15.05.2021).

¹³ Ситников Е. С. Правовой режим криптовалют в России // Novaum. 2018. № 13. С. 148–149.

финансовыми активами. К нему предъявляется ряд требований, при соблюдении которых он может подать заявление и встать на учёт в реестре операторов обмена цифровых финансовых активов.

Рассмотрим требования в ст. 3 ФЗ «О цифровых финансовых активах», предъявляемые к *решению* для выпуска цифровых финансовых активов в операторе информационной системы. *Решение* должно содержать: сведения о лице, выпускающем цифровые финансовые активы, сведения об операторе информационной системы, в которой осуществляется выпуск цифровых финансовых активов, количество выпускаемых цифровых финансовых активов, цену их приобретения и дату начала их размещения. Решение должно быть размещено в информационно-телекоммуникационной сети Интернет и признается публичной офертой.

Данные требования являются противоречивыми по отношению к идее криптовалюты, которая гарантирует анонимность её владельцам. С первого и до конечного этапа обмена и выпуска цифровой валюты её владелец сообщает практически всю информацию о себе. Таким образом, игнорируется и уничтожается специфика криптовалюты как таковой. Этот фактор, а также большое количество требований, предъявляемых к участникам оборота и управленческому составу оператора информационной системы, являются

препятствием для комфортного и свободного оборота криптовалюты в России, так как по сути законодатель устанавливает правовой режим, который криптовалюта избегает в силу своей специфики (децентрализованность, анонимность, автономность и т. д.). Законодатель желает строго регулировать данную деятельность, так как возникает опасность финансирования терроризма, проблема налогообложения владельцев цифровых финансовых активов и возможность отмыwania нелегальных доходов через данный механизм¹⁴. Поэтому необходимо найти компромисс, который позволит стимулировать оборот криптовалюты без нанесения ущерба национальной финансовой системе и государственной безопасности России.

Одним из таких вариантов является сохранение анонимности для пользователей относительно оператора обмена цифровых финансовых активов и остальных пользователей. Данная процедура может осуществляться следующим образом: участники оборота криптовалюты обязаны получить лицензию на осуществление данной деятельности; лицензия выдается соответствующим государственным органом; при ее получении участники вносят свои личные данные (п. 1 ст. 3 ФЗ «О цифровых финансовых активах»), которые становятся конфиденциальными. Эта процедура становится допуском для осуществления деятельности по

¹⁴ Лютова О. И. Определение понятия криптовалюты для целей налогово-

правового регулирования // Теология. Философия. Право. 2019. № 1 (9). С. 19–26.

обороту цифровых финансовых активов. Данные, указанные пользователем информационной системы, сохраняются у органа, который выдает лицу лицензию, и не разглашаются. При регистрации пользователя в информационной системе ему присваивается идентификационный номер. Обмен и выпуск цифровых финансовых активов должен производиться по назначенному номеру. Таким образом, можно легко отследить все транзакции, производимые между участниками оборота цифровых финансовых активов, цену их приобретения и дату размещения криптовалюты. При этом сохраняется анонимность участников как для оператора обмена цифровых финансовых, так и для остальных его пользователей. Налогообложение по данной деятельности возможно осуществлять так же, как при обороте ценных бумаг (размер налога включается в комиссию во время произведения обмена, продажи или выпуска цифровых финансовых активов). При обнаружении обстоятельств, которые могут характеризоваться как потенциально опасные (подозрение в финансировании терроризма или в возможности отмыwania доходов), соответствующий государственный орган может через решения суда раскрыть данные о лице и о подробностях его деятельности и начать расследование. В приведенном варианте, лицо, осуществляющее обмен и выпуск цифровых

финансовых активов, сохраняет свою анонимность при добросовестном осуществлении данной деятельности. В век информатизации одной из угроз является проблема защиты частной жизни. Именно криптовалюта гарантирует защиту персональных данных и охрану личной жизни, что и является ее уникальной чертой.

Исходя из полученной информации о странах с *дозволительной* моделью правового регулирования мы можем выделить признаки этой модели: разрешение операций с криптовалютой, контроль государства над этими операциями и создание специальных платформ для обеспечения обмена криптовалюты. В июле в РФ вышел ФЗ «О цифровых финансовых активах», который разрешает отношения при выпуске и обращении цифровых финансовых активов, вводит определенные требования к участникам оборота и устанавливает порядок создания оператора обмена цифровых финансовых активов. Таким образом, можно сделать вывод о переходе РФ к дозволительной модели правового регулирования криптовалюты. Но несмотря на это обстоятельство на сегодняшний день на территории России не зарегистрирован ни один оператор обмена цифровых финансовых активов: об этом свидетельствует реестр, расположенный на сайте Центрального Банка России¹⁵. Это указывает на существующие препятствия, которые стоят перед потенциальными участниками

¹⁵ Центральный Банк России URL: https://www.cbr.ru/finm_infrastructure/otsfa/ (дата обращения: 15.05.2021).

оборота криптовалюты и не позволяют комфортно реализовывать данную деятельность. Поэтому необходимо обратить внимание на изменение правового режима криптовалюты в Российской Федерации: с правового режима, который полностью раскрывает

информацию о владельцах криптовалюты, на правовой режим, при котором сохраняется их анонимность. Это позволит в дальнейшем повысить уровень развития криптовалюты, технологического прогресса и инвестиционной привлекательности.

Список литературы

1. Аманжолова Б. А. Правовое регулирование криптовалют в мире // Образование и право. 2018. № 5. С. 228–231.
2. В каких странах запрещено использовать Биткоин // Портал finswin.com. URL: <https://finswin.com/kripto/btc/gde-zapreshchen-bitkoin.html>.
3. Глобенко О. А. Криптовалюта: проблемы правового регулирования и доктринального определения / О. А. Глобенко, А. А. Ильягуева // Образование и право. 2018. № 3. С. 135–140.
4. Лютова О. И. Определение понятия криптовалюты для целей налогово-правового регулирования // Теология. Философия. Право. 2019. № 1 (9). С. 19–26.
5. Середа А. В. Зарубежный опыт правового регулирования оборота виртуальных валют: модели и подходы / А. В. Середа, Г. Ф. Ручкина // Образование и право. 2019. № 7. С. 99–103.
6. Ситников Е. С. Правовой режим криптовалют в России // Novaum. 2018. № 13. С. 148–149.
7. Chan E. China Plans to Ban Cryptocurrency Mining in Renewed Clampdown // Bloomberg. URL: <https://www.bloomberg.com/news/articles/2019-04-09/china-plans-to-ban-cryptocurrency-mining-inrenewed-clampdown>.
8. Čiulada P. Lietuvos bankas apsisprendė dėl bitkoinų // Verslo žinios. URL: <https://www.vz.lt/archive/article/2014/1/31/lietuvos-bankas-perspeja-del-bitkoinu>.
9. Dewey J. Global Legal Insights: Blockchain & Cryptocurrency Regulation // The Association of Corporate Counsel. URL: https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf.
10. Press Release. Bank of Lithuania. Bank of Lithuania Announces Its Position on Virtual Currencies and ICO (Oct. 11, 2017) // Bank of Lithuania: official site. URL: <https://www.lb.lt/en/news/bank-of-lithuania-announces-its-positionon-virtual-currencies-and-ico>.

Vladislav D. Gridasov
Student,
Ural State Law University
(Yekaterinburg, Russian Federation)
slawa.gridasov@yandex.ru

Scientific supervisor – E. V. Dzhenakova, Senior Lecturer of the Department of
Information Law

CHANGING THE LEGAL REGIME OF CRYPTOCURRENCY IN RUSSIA BASED ON FOREIGN EXPERIENCE

Abstract: In 2009, a new technology appeared – cryptocurrency. Due to its specific features, many countries have different approaches to the legal regulation of cryptocurrency. Its general international legal regime has not yet been defined, nor have uniform international standards and rules been established to unify the mechanism of legal regulation of cryptocurrency. This problem leads to a restriction of the turnover of the cryptocurrency and its development. This article examines the various mechanisms (models) of legal regulation of virtual currencies that exist in the modern world. Based on their analysis, one of the options for changing the legal regime of cryptocurrency in Russia is proposed.

Keywords: cryptocurrency, digital financial assets, legal regulation models, virtual currency, turnover.

УДК 342.82

Гурьева Екатерина Евгеньевна

Студент,

Волго-Вятский институт (филиал)

Университета имени О. Е. Кутафина (МГЮА)

(г. Киров, Российская Федерация)

ekaterina.gureva01@gmail.com

Научный руководитель – И. А. Пибаетов, кандидат юридических наук, доцент
кафедры государственно-правовых дисциплин

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ «БЛОКЧЕЙН» В ИЗБИРАТЕЛЬНОМ ПРОЦЕССЕ

Аннотация: В данной статье рассматривается вопрос о возможности применения технологии «блокчейн» в избирательном процессе Российской Федерации. В настоящей работе проанализирован механизм функционирования данной технологии, на основе этого выявлены положительные аспекты применения блокчейна на выборах. Также приводятся примеры использования данной технологии в различных сферах и в зарубежных странах. Особое внимание уделяется рискам и проблемам, которые могут возникнуть при внедрении блокчейн-технологии в избирательный процесс в Российской Федерации.

Ключевые слова: блокчейн, избирательный процесс, голосование, выборы, криптография, информационные технологии.

Для цитирования:

Гурьева Е. Е. Использование технологии «блокчейн» в избирательном процессе // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 157–167.

Право избирать и быть избранным в органы государственной власти и органы местного самоуправления, закрепленное в части 2 статьи 32 Конституции Российской Федерации, относится к основополагающим конституционным правам граждан Российской Федерации, и от того насколько полно оно может быть реализовано, зависит как легитимность власти в целом, так и уровень демократии в стране. Для

успешного функционирования современного демократического государства огромное значение имеют открытые выборы и, соответственно, обеспечение их прозрачности различными институтами и правовыми инструментами. Граждане Российской Федерации не должны сомневаться в законности выборов, так как это приводит к снижению явки избирателей на выборы, а также к недоверию к кандидатам и к действующей власти в целом. В связи

с этим стоит вопрос о необходимости цифровизации электорального процесса в России; внедрение новых технологий при правильном их применении может обеспечить прозрачность выборов и невозможность вмешательства третьих лиц в избирательный процесс.

Так, в Российской Федерации уже достаточно давно действует государственная автоматизированная система «Выборы». В 2003 году появились первые комплексы обработки избирательных бюллетеней, а в 2011 году были разработаны комплексы электронного голосования, на основе которых впоследствии были созданы специальные сенсорные карты. Суть функционирования данной системы заключается в том, что сетевой контроллер, который управляет базой данных, собирает информацию со всех подключенных комплексов электронного голосования, а само голосование осуществляется посредством специальных кодов. Положительным моментом является то, что ГАС «Выборы» формирует и обеспечивает актуальность базы данных об избирателях, а также гарантирует обмен информацией между избирательными комиссиями различных уровней.

Особое место среди инновационных технологий, которые можно применить в избирательном процессе, занимает технологическая разработка «блокчейн». Данная

технология является универсальной, так как она может применяться практически во всех сферах жизнедеятельности. Например, данная технология активно используется в банковской деятельности, посредством системы «блокчейн» информация о всех банковских операциях сохраняется на специальных банковских серверах. Таким образом, банк при применении данной технологии может сохранять конфиденциальность данной информации и распоряжаться сбережениями физических и юридических лиц, добровольно передавших их на хранение, в своих интересах, при этом не ставя их в известность. По мнению директора ПАО «Сбербанк» Г.О. Грефа, применение технологии «блокчейн» со временем может привести к упразднению большинства банков не только в России, но и во всём мире. В силу этого обстоятельства он рекомендует банкам уже сейчас активно использовать технологию «блокчейн» в своей деятельности¹. О популярности данной технологии в современном мире свидетельствует и тот факт, что ведущие банки во всём мире запускают свои криптовалюты. Например, с марта 2018 года Австралийская фондовая биржа перешла на технологию «блокчейн» для хранения данных об участниках биржевых торгов, о заключаемых

¹ Алексеев Р. А. Блокчейн как избирательная технология нового поколения – перспективы применения на выборах в современной России // Вестник Московского государственного областного университета.

2018. № 2. С. 3–10. Режим доступа: Научная электронная библиотека Elibrary.ru. URL: <https://elibrary.ru/item.asp?id=35395209> (дата обращения: 01.05.2021).

сделках и проведении платежей по контрактам².

Также данная технология может применяться и в сфере здравоохранения, где вся информация вместо медицинских карт, в которые вносится история болезни пациента будет храниться в системе «блокчейн».

Основным преимуществом является то, что данную информацию невозможно будет подделать или изменить, это будет касаться и неверных диагнозов, и различных врачебных ошибок. Технологию «блокчейн» можно внедрять и в сферу логистики, благодаря этому для потребителей станет абсолютно прозрачной информация, влияющая на его конечную стоимость, касающаяся доставки товаров, их производства и сроков хранения.

Компания IBM в США призывает государственные структуры к применению во властно-управленческой деятельности облачных технологий, а в частности технологии на основе платформы «блокчейн», поскольку это сможет обеспечить экономию как времени, так и бюджетных средств³.

Теперь обратимся непосредственно к описанию технологии «блокчейн». Данная технология представляет собой децентрализованную открытую базу данных, распределенную между всеми участниками сети, которая используется для различных операций

между этими участниками. Такое понимание технологии «блокчейн» основано на определении ее создателя – Сатоши Накамото. По его мнению, и технология блокчейн, и лежащий в ее основе «биткоин» представляет собой основанную на шифровании систему, а именно механизм создания цепочки из блоков информации, в которых содержатся сведения о совершении всех операций с начала функционирования первого блока данной цепочки. Соединение всех блоков в единую цепь доказательств проведения сложных математических вычислений каждым участником такой цепи и служит гарантией недопустимости крэкинга и присоединения «неверных» блоков, которые не учитывают совершение всех предыдущих операций, поскольку цепочка остается непрерывной и в ней хранится информация обо всех операциях, проведенных с момента ее создания. Следовательно, чтобы провести в этой сети новую операцию, нужно обязательно получить отклик от каждого узла цепи, находящегося в данный момент в системе, то есть как бы «нарастить» уже существующую цепь блоков информации новым, информацию о котором, при этом получают все узлы сети и автоматически подтверждают ее, если она не содержит признаков взлома.

В качестве блока информации может выступать, например, новая единица цифровой валюты – биткоин

² Как голосование на блокчейне находит свое применение в политике и бизнесе // Хабр. Дата обновления: 28.11.2016. URL: <https://habr.com/ru/company/wirex/blog/398125/> (дата обращения: 28.04.2021).

³ Федорченко С. Н., Федорченко Л. В. Власть и облачные технологии в России и США // Вестник Московского государственного областного университета. Серия: История и политические науки. 2016. № 2. С. 108–116.

или другая ценная единица, в том числе такой единицей может быть и голос избирателя. После того как подобный блок был создан и подтвержден остальными узлами цепи, в него уже невозможно внести изменения или удалить его. Также стоит отметить, что информация обо всей цепочке постоянно открыта для всех участников, которые при желании могут отследить каждую операцию, не видя персональных данных конкретных лиц. Можно сказать, что «блокчейн» – это своеобразный открытый электронный регистрационный журнал, в который вносятся необходимые данные. Например, в случае с биткоином этими данными являются сведения о транзакциях между пользователями криптовалюты.

Благодаря описанным выше принципам функционирования данная технология имеет ряд преимуществ, которые доказывают возможность эффективного применения данной технологии в избирательном процессе. Так, при голосовании с использованием технологии «блокчейн» достигается и обеспечивается:

во-первых, убедительность доказательства легитимности процедуры голосования;

во-вторых, прочная гарантия от внедрения в цепь связанных блоков информации, узлов блока контрафактной транзакции⁴;

в-третьих, анонимность личности избирателя, соответственно, соблюдение принципа тайного волеизъявления, а также отсутствие необходимости внешнего контроля за ходом голосования.

Описание процедуры выборов с использованием данной технологии было дано Д. Тапскоттом. По его мнению, при голосовании с использованием системы «блокчейн» бюллетень, получаемый избирателем, соответствует цифровой монете, достоинство которой соотносится с уровнем выборов. Гражданин размещает данную монету в кошельке кандидата, выбранного избирателем, тем самым, реализует активное избирательное право через аутентификацию самого себя на виртуальной платформе «блокчейн», которая проводит суммирование поданных голосов и подтверждает правильность учёта волеизъявления каждого участника голосования⁵.

Блокчейн характеризуется наличием так называемого «протокола правды», который позволяет проводить безопасное голосование в цифровой форме. Согласно заключению экспертного сообщества Испании, фактор применения нового способа голосования с использованием блокчейн-технологии подтверждает смещение предпочтений в выборе учёта подаваемых голосов: от централизованного порядка суммирования голосов избирателей к

⁴ Гилбурт В. От бюллетеней к биткоину: как блокчейн изменил государство // BitNovosti. Дата обновления: 31.08.2015. URL: <http://bitnovosti.com/2015/08/31/ballot-box-bitcoin> (дата обращения: 28.04.2021).

⁵ Тапскотт Д. Технология блокчейн: то, что движет финансовой революцией сегодня. Москва: Эксмо, 2017. 448 с.

децентрализованному реестру голосов на платформе блокчейна. Данное заключение является сущностной оценкой технологии блокчейн-голосования, признанием ценности демократии и важности гарантированной защиты и обеспечения реализации избирательных прав граждан в условиях преобразований в информационном обществе.

Технология блокчейн-голосования, которую можно отнести к разряду «техно-демократических», позволит обеспечить необходимый уровень согласованности между обществом и государственной властью. Следовательно, данное обстоятельство определяет конституционно-правовой характер целесообразности технического переоборудования избирательной системы и преимущества реализации новой технологии «блокчейн» перед существующими в настоящее время способами голосования.

Следует заметить, что во многих зарубежных странах технология «блокчейн» уже давно используется в различных форматах при проведении выборов. Например, в США был разработан и реализован проект FollowMyVote на платформе «блокчейн». Апробация данного проекта была произведена с 23 марта по 8 мая 2018 года при организации голосования на предварительных выборах для военнослужащих,

находящихся за рубежом. Технология онлайн-голосования на платформе «блокчейн» была применена в избирательных округах штата Западная Вирджиния. Основу криптографии проекта FollowMyVote составляет метод эллиптической кривой, который гарантирует надежную защиту блоков информации, находящихся в цепи. При этом программное обеспечение системы «блокчейн» построено по принципу открытого исходного кода, следовательно, этот вид кода способствует сквозной верификации блочной цепи на всём её протяжении⁶.

В Греции была разработана система DEMOS, представляющая собой распределенный реестр публичного характера типа «блокчейн», который создает цифровую корзину для бюллетеней, при этом граждане могут воспользоваться данной системой из любой точки мира. Проголосовав, избиратели получают специальные коды – наборы чисел, с помощью которых они могут проверить, действительно ли голос отдан за кандидата, которого они предпочли, а также узнать время передачи голоса и его учета при подсчете⁷.

Отдельного внимания заслуживает проведение блокчейн-эксперимента в Сьерра-Леоне на выборах президента 7 марта 2018 года. Швейцарский фонд «Agora» предложил Национальному

⁶ Follow My Vote, Inc. // Roanoke-Blacksburg Technology Council, RBTC. [website]. URL: <https://rbtc.tech/Members/#!/biz/id/54f4e0b39857ec135106e7ff/About> (accessed: 28.04.2021).

⁷ «Выборы на блокчейне»: как это работает и что дает избирателям // Рамблер.Новости.

Дата обновления: 18.10.2017. URL: <https://news.rambler.ru/other/38181945-vybory-na-blokcheyne-kak-eto-rabotaet-i-chto-daet-izbiratelyam/> (дата обращения: 28.04.2021).

избирательному комитету Сьерра-Леоне экспериментальный подсчет голосов избирателей посредством новой технологии блокчейн-голосования на платформе распределенных реестров публичного характера. Важно отметить, что достоинством использования данной технологии при проведении голосования является прозрачность производимых транзакций при помощи *cryptocurrency* и использования публичных реестров, записывающих по принципу блокчейна каждый голос⁸. Более того, произведенные записи может просматривать каждый заинтересованный человек, но при этом проводить верификацию отданных голосов могут только уполномоченные лица. По мнению генерального директора фонда «Agora» Леонардо Гаммара, новая блокчейн-технология препятствует применению манипулятивных действий со стороны правящей партии и способствует обеспечению этнической лояльности для отдельных групп электората. Кроме того, технология электронного подсчета голосов на платформе блокчейна является наиболее приемлемой для

бедных стран по причине экономии бюджетных средств, выделяемых на изготовление традиционных бумажных бюллетеней. Важно заметить, что пилотный вариант новой технологии был реализован для страны с низким уровнем грамотности населения, плохой сетевой связанностью, и случаями электорального принуждения в виде «частого насилия на выборах»⁹.

Согласно мнению операционного директора «Agora» Я. Лукасевича, новая технология «блокчейн» имеет явно выраженное будущее для своего применения и в настоящее время является единственной технологией, способной к практической реализации «прозрачной платформы для доказуемо честных выборов»¹⁰.

В Российской Федерации также были попытки внедрения блокчейн-технологии в электоральный процесс, но они не обеспечили реализации отмеченных выше преимуществ технологии «блокчейн». Так, на выборах в Московскую городскую думу 2019 года использовалась платформа «блокчейн» закрытого типа¹¹, что в итоге стало причиной возникновения ряда негативных

⁸ Чимаров Н. С. К вопросу о первом опыте применения новых технологий голосования на выборах президента страны: блокчейн-эксперимент в Сьерра-Леоне // Человек и закон: Актуальные вопросы, достижения и инновации: материалы II Международной научно-практической конференции. Пенза: Наука и Просвещение, 2018. С. 20–22. Режим доступа: Научная электронная библиотека Elibrary.ru. URL: <https://elibrary.ru/item.asp?id=35549456&pff=1> (дата обращения: 01.05.2021).

⁹ Kazeen Y. The world's first blockchain supported elections just happened in Sierra

Leone // Quartz Media. Updated: 13.03.2018. URL: <https://qz.com/1227050/sierra-leone-elections-powered-by-blockchain> (accessed: 28.04.2021).

¹⁰ Castillo M. Sierra Leone Secretly Holds First Blockchain-Audited Presidential Vote // Coindesk. Updated: 20.03.2018. URL: <https://www.coindesk.com/sierra-leone-secretly-holds-first-blockchain-powered-presidential-vote> (accessed: 29.04.2021).

¹¹ Электронные выборы в Московскую городскую Думу // Официальный портал Мэра и Правительства Москвы. URL:

последствий. В частности, возникла проблема непредоставления доступа к той информации, которая должна быть открытой, а также большое количество технических неполадок и сбоев. Вследствие чего появились сомнения в демократичности состоявшегося голосования. Поэтому для избежания подобных ситуаций необходимо использовать открытые блокчейн-платформы, информация об операциях в которых носит общедоступный характер.

По заявлению Председателя ЦИК России Э. Ю. Памфиловой, тестирование отечественной системы блокчейн-голосования планируется провести в 2024 г. на выборах Президента Российской Федерации. Разрабатываемый в настоящее время отечественный проект применения распределённого реестра голосования на платформе блокчейна должен отвечать критериям беспрецедентной транспарентности и защищенности, подтверждая при этом полную легитимность проведённых избирателем на интернет-платформе действий¹².

Представляется, что технология «блокчейн» может быть внедрена на выборах в Российской Федерации при проведении голосования. При этом процедура голосования будет состоять в следующем: каждый избиратель в день голосования в отведенный промежуток времени авторизуется на специальной интернет-платформе (для этих целей можно использовать портал «Госуслуги» или раздел в ГАС

«Выборы»), затем избиратель выбирает раздел для голосования на выборах соответствующего уровня и путем выбора понравившегося кандидата или списка, выдвинутого избирательным объединением, голосует, нажав соответствующую кнопку на данной платформе (портале или сайте). После этого происходит мгновенная автоматическая отправка сведений о голосе через распределённый реестр информации о голосовании всех избирателей в избирательную комиссию, причем на федеральных выборах голоса могут сразу направляться в Центральную избирательную комиссию Российской Федерации, минуя территориальные избирательные комиссии и избирательные комиссии субъектов Российской Федерации. В последующем, когда время голосования заканчивается, избирательная комиссия автоматически формирует протокол об итогах голосования и оглашает его. Такой подход практически исключает возможность искажения результатов реального волеизъявления избирателей, т. к. система является децентрализованной и на нее не получится повлиять из какого-либо отдельного центра.

Помимо непосредственно голосования технология «блокчейн» может применять и на других стадиях избирательного процесса. Например, данная технология может стать способом реализации такой формы поддержки выдвижения кандидатов,

<https://www.mos.ru/city/projects/blockchain-vybory/> (дата обращения: 28.04.2021).

¹² Сабиров О. Глава ЦИК: система выборов на блокчейна появится в России в

ближайшие четыре года // 2Bitcoins.ru. URL: <https://2bitcoins.ru> (дата обращения: 29.04.2021).

как сбор подписей избирателей. Предлагается реализовать механизм на специальной платформе (или через тот же портал «Госуслуги»), предоставив каждому авторизованному и подтвердившему свою личность гражданину возможности поддержать кандидата посредством голосования за него через интернет-платформу, информация с которой посредством блокчейн-технологии будет передаваться в избирательную комиссию, организующую выборы. Такая форма поддержки выдвижения кандидатов позволяет решить ряд проблем со сбором подписей на бумажных носителях: во-первых, пропадает необходимость тщательной проверки каждого подписного листа, на что тратятся ресурсы как самого кандидата, так и избирательных комиссий, во-вторых, снимаются все споры о подлинности подписей избирателей в подписном листе, а также о правильности его заполнения, если предусмотреть автоматическое заполнение всех данных после авторизации избирателя в разделе для голосования, исходя из персональных данных, представленных им при регистрации на интернет-платформе.

При этом, несмотря на ряд неоспоримых преимуществ применения технологии «блокчейн» при проведении выборов, стоит отметить и проблемы, которые могут возникнуть при реализации голосования с помощью данной технологии. Во-первых, защищенность системы от контрафактного изменения, удаления или добавления блоков информации не может гарантировать

невозможность кракинга или иного постороннего воздействия посредством использования ошибочного или вредоносного программного обеспечения на электронных устройствах избирателей. Во-вторых, возникает риск неисправимости технически ошибочно поданного избирателем своего голоса, то есть невозможность внесения изменений после отправки. В-третьих, может создаваться угроза мощностям национальной энергетической системы по причине чрезвычайно большого потребления энергии системами включённого блокчейн-голосования при многомиллионной численности избирателей.

Также при применении блокчейн-платформ возникает проблема нарушения важнейших принципов избирательного права, таких как всеобщее и равное голосование, свобода волеизъявления гражданина на выборах, тайное голосование, гласность и открытость выборов. Так, например, хоть и существует возможность принять участие в выборах не выходя из дома или находясь в любой точке мира, но при этом возникает проблема гарантированности самостоятельности голосования избирателя, без какого-либо давления, ведь попасть к избирателю и воздействовать на него будет проще, чем на избирательном участке при традиционной процедуре голосования, так как там присутствуют наблюдатели и сотрудники полиции. Следовательно, ставится под сомнение свобода волеизъявления гражданина при

выборе того или иного кандидата и тайна голосования в целом. Кроме того, при использовании подобного способа голосования достаточно сложно обеспечить наблюдение за выборами, соответственно, это может привести к нарушению принципа гласности и открытости выборов. Также возникает проблема обеспечения равенства возможностей для участия в выборах, поскольку далеко не у всех граждан есть устройства с возможностью выхода в сеть Интернет, поэтому для обеспечения принципа всеобщности голосования необходимо комбинировать голосование на платформе «блокчейн» с традиционным способом голосования на избирательном участке.

Подводя итог, можно с уверенностью говорить о возможности эффективного применения инновационных технологических разработок при проведении выборов в Российской

Федерации, а именно технологии «блокчейн». Данную технологию можно использовать на различных стадиях избирательного процесса, механизм функционирования системы «блокчейн» позволяет гарантировать безопасность и защищенность от «вброса голосов» и различного рода фальсификаций, а также прозрачность и открытость голосования, сохраняя при этом тайну голосования избирателя. Несмотря на ряд положительных аспектов, существуют и определенные риски применения технологии «блокчейн» при проведении выборов, которые могут повлечь нарушение основных принципов избирательного права. Поэтому при внедрении данной технологии в электоральный процесс предлагается совмещение нововведений с традиционными способами голосования в целях недопущения нарушения основополагающих принципов.

Список литературы

1. ««Выборы на блокчейне»: как это работает и что дает избирателям» // Рамблер.Новости. Дата обновления: 18.10.2017. URL: <https://news.rambler.ru/other/38181945-vybory-na-blokcheyne-kak-eto-rabotaet-i-chto-daet-izbiratelyam/>.
2. Алексеев Р. А. Блокчейн как избирательная технология нового поколения – перспективы применения на выборах в современной России // Вестник Московского государственного областного университета. 2018. № 2. С. 3–10. Режим доступа: Научная электронная библиотека Elibrary.ru. URL: <https://elibrary.ru/item.asp?id=35395209>.
3. Гилбурт В. От бюллетеней к биткоину: как блокчейн изменил государство // BitNovosti. Дата обновления: 31.08.2015. URL: <http://bitnovosti.com/2015/08/31/ballot-box-bitcoin>.
4. Как голосование на блокчейне находит свое применение в политике и бизнесе // Хабр. Дата обновления: 28.11.2016. URL: <https://habr.com/ru/company/wirex/blog/398125/>.

5. Сабиров О. Глава ЦИК: система выборов на блокчейна появится в России в ближайшие четыре года // 2Bitcoins.ru. URL: <https://2bitcoins.ru>.
6. Тапскотт Д. Технология блокчейн: то, что движет финансовой революцией сегодня. Москва: Эксмо, 2017. 448 с.
7. Федорченко С. Н. Власть и облачные технологии в России и США / С. Н. Федорченко, Л. В. Федорченко // Вестник Московского государственного областного университета. Серия: История и политические науки. 2016. № 2. С. 108–116.
8. Чимаров Н. С. К вопросу о первом опыте применения новых технологий голосования на выборах президента страны: блокчейн-эксперимент в Сьерра-Леоне // Человек и закон: Актуальные вопросы, достижения и инновации: материалы II Международной научно-практической конференции. Пенза: Наука и Просвещение, 2018. С. 20–22. Режим доступа: Научная электронная библиотека Elibrary.ru. URL: <https://elibrary.ru/item.asp?id=35549456&pff=1>.
9. Электронные выборы в Московскую городскую Думу // Официальный портал Мэра и Правительства Москвы. URL: <https://www.mos.ru/city/projects/blockchain-vybory/>.
10. Castillo M. Sierra Leone Secretly Holds First Blockchain-Audited Presidential Vote // Coindesk. Updated: 20.03.2018. URL: <https://www.coindesk.com/sierra-leone-secretly-holds-first-blockchain-powered-presidential-vote>.
11. Follow My Vote, Inc. // Roanoke-Blacksburg Technology Council, RBTC. [website]. URL: <https://rbtc.tech/Members/#!/biz/id/54f4e0b39857ec135106e7ff/About>.
12. Kazeen Y. The world's first blockchain supported elections just happened in Sierra Leone // Quartz Media. Updated: 13.03.2018. URL: <https://qz.com/1227050/sierra-leone-elections-powered-by-blockchain>.

Ekaterina E. Gurieva

Student,

Volga-Vyatka Institute (branch) of Kutafin Moscow State Law University (MSAL)

(Kirov, Russian Federation)

ekaterina.gureva01@gmail.com

Scientific supervisor – I. A. Pibaev, PhD (Law), Associate Professor of the Department of State and Legal Disciplines

BLOCKCHAIN TECHNOLOGY IN THE ELECTORAL PROCESS

Abstract: This article discusses the possibility of using the blockchain technology in the electoral process of the Russian Federation. In this paper, the mechanism of functioning of this technology is analyzed, and on the basis of this, positive aspects of the use of blockchain in elections are identified. Examples of the use of this technology in various fields and in foreign countries are also given. Special attention is paid to the risks and problems that may arise when implementing blockchain technology in the electoral process in the Russian Federation.

Keywords: blockchain, electoral process, voting, elections, cryptography, information technologies.

УДК 343.98

Гусейнов Рамиль Гахраманович

Студент,
Уральский государственный юридический университет
(г. Екатеринбург, Российская Федерация)
grg1203@bk.ru

Стренин Данил Алексеевич

Студент,
Финансовый университет при Правительстве Российской Федерации
(г. Москва, Российская Федерация)
strenin@mail.ru

Курилюк Юлия Евгеньевна

Кандидат юридических наук, доцент департамента международного и публичного права,
Финансовый университет при Правительстве РФ
(г. Москва, Российская Федерация)
kat-serebr@mail.ru

ЦИФРОВЫЕ ПЛАТФОРМЫ КАК МЕХАНИЗМ ОБЕСПЕЧЕНИЯ РОСТА ЦИФРОВОЙ ЭКОНОМИКИ РОССИИ

Аннотация: В цифровой экономике объемы производства существенно возрастают, требуя при этом ускорения процессов заключения сделок. Заключение договоров купли-продажи через цифровые платформы способно удовлетворить современные запросы общества, расходуя меньшее количество товаров на доставку и реализацию товаров. В статье анализируются изменения на рынке, которые должны произойти с принятием Закона «О цифровых правах».

Ключевые слова: цифровые платформы, потребитель, купля-продажа, электронные сделки, цифровые права.

Для цитирования:

Гусейнов Р. Г. Цифровые платформы как механизм обеспечения роста цифровой экономики России / Р. Г. Гусейнов, Д. А. Стренин, Ю. Е. Курилюк // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 168–171.

Капитализация компаний, использующих цифровые платформы, по состоянию на 2019 год в несколько раз превышает капитализацию производственных хозяйственных обществ. Это объясняется экономической выгодой платформенного бизнеса как для потребителей, так и для продавцов. И со вступлением в силу с 1 октября

2019 года «Закона о цифровых правах» в Российской Федерации платформенный бизнес должен активно начать развиваться в связи с внедрением электронных средств платежа, в том числе и в регионах.

Цифровые платформы коренным образом изменяют традиционные модели ведения бизнеса и поведения потребителей. Ведь цифровой канал распределения товаров и услуг связывает напрямую производителей и потребителей через прямые каналы сбыта, что устраняет посреднические звенья, снижает при этом издержки бизнеса.

«Закон о цифровых правах» приравнивает сделки в электронной форме к сделкам, совершенным в письменной форме¹, что гарантирует «электронным договорам» все средства защиты, а также должно повысить их использование у массового потребителя.

Активным представителем платформенной экономики является китайская компания Alibaba group, анализ которой позволит выявить позитивные и негативные аспекты цифровых платформ и возможности их применения в Российской Федерации. Возможностями Alipay по оплате товаров и услуг регулярно пользуются более 80 % владельцев мобильных устройств в Китае, ведь крупнейшие банки КНР уделяют мало внимания клиентскому сервису.

Российским банкам следует исходить из китайского опыта и вкладывать необходимое финансирование в развитие сервиса электронного обслуживания клиентов, чтобы быть конкурентоспособными по отношению к таким цифровым моделям, как Alipay.

Применение цифровых платформ² снижает затраты на маркетинг, увеличивая, в свою очередь, объемы рынка: появляется адаптивная информация о предпочтениях потребителей. В частности, сотрудники Alibaba group используют Большие данные для анализа поведения потребителей, создавая рейтинги ненадежных продавцов. На данный момент банк ВТБ также старается внедрять Big Data, однако использует их только для ускорения обработки информации, что не раскрывает полностью потенциал данной технологии.

Более 90 % транзакций посредством цифровых платформ осуществляются безналичным способом, что облегчает деятельность налоговым органам, поскольку расчеты между продавцами и потребителями становятся прозрачными³.

Государство должно создать «единые правила игры» и вести разумный цифровой протекционизм. Ведь, анализируя практику осуществления деятельности

¹ Гражданский кодекс Российской Федерации (часть первая): федеральный закон № 51-ФЗ (ред. от 08.12.2020) от 30.11.1994 // Собрание законодательства РФ. 1994. № 32. Ст. 3301.

² Федеральный закон № 34-ФЗ от 18.03.2019 «О внесении изменений в части первую, вторую и статью 1124 части третьей

Гражданского кодекса Российской Федерации» // Собрание законодательства РФ. 2019. № 12. Ст. 1224.

³ Купревич Т. С. Цифровые платформы в мировой экономике: современные тенденции и направления развития // Экономический вестник университета. 2017. № 37. С. 311–318.

китайской цифровой платформы Alibaba Group, следует отметить, что в Российской Федерации создаются условия для осуществления электронных транзакций, благодаря введению цифровых прав и цифровых денег, что повышает привлекательность данного сегмента рынка для инвесторов. Также государству необходимо гарантировать исполнение обязательств в цифровой среде с

целью повышения доверия потребителей к цифровым платформам.

Таким образом, цифровые платформы появляются в традиционных сферах предпринимательской деятельности и приводят к инновациям, что способно изменить поведение потребителей на рынке и способы выражения ими своей воли.

Список литературы

1. Купревич Т. С. Цифровые платформы в мировой экономике: современные тенденции и направления развития // Экономический вестник университета. 2017. № 37. С. 311–318.

Ramil G. Guseynov

Student,

Ural State Law University
(Yekaterinburg, Russian Federation)
grg1203@bk.ru

Danil A. Strenin

Student,

Financial University under the Government of the Russian Federation
(Moscow, Russian Federation)
strenin@mail.ru

Yulia Y. Kurylyuk

PhD (Law), Associate Professor of the Department of International and Public Law,
Financial University under the Government of the Russian Federation
(Moscow, Russian Federation)
kat-serebr@mail.ru

DIGITAL PLATFORMS AS A MECHANISM FOR ENSURING THE GROWTH OF THE DIGITAL ECONOMY OF RUSSIA

Abstract: In the digital economy, production volumes are significantly increasing, while requiring the acceleration of transaction processes. The conclusion of purchase and sale contracts through digital platforms is able to meet the modern demands of society,

III. Распределённый реестр, смарт-контракты, криптовалюты и иные цифровые продукты

spending less on the delivery and sale of goods. The article analyzes the changes in the market that should occur with the adoption of the Law «On Digital Rights».

Keywords: digital platforms, consumer, purchase and sale, electronic transactions, digital rights.

Мелентьева Валерия Валерьевна

Студент,

Северный (Арктический) федеральный университет им. М. В. Ломоносова
(г. Архангельск, Российская Федерация)

melentiewa.valeria@yandex.ru

Научный руководитель – С. Е. Жура, кандидат экономических наук,
исполняющий обязанности заведующего кафедрой финансового права и
правоведения, доцент кафедры финансового права и правоведения

РАЗВИТИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ КРИПТОВАЛЮТЫ: ОПЫТ РОССИИ И ЗАРУБЕЖНЫХ СТРАН

Аннотация: Статья посвящена анализу правового положения криптовалюты в России и зарубежных странах: США, Германии, Швейцарии, Японии, Австралии. Указывается на полярность во взглядах государственных властей по поводу легализации использования цифровых финансовых активов. Рассмотрены позиции судов Российской Федерации в отношении виртуальной валюты, выяснено, что дела, связанные с использованием цифровых денежных средств, на данный момент разрешаются на основе судебного усмотрения.

Ключевые слова: криптовалюта, блокчейн-технология, цифровые финансовые активы, правовое регулирование, виртуальная валюта, средства платежа, цифровые права.

Для цитирования:

Мелентьева В. В. Развитие правового регулирования криптовалюты: опыт России и зарубежных стран // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 172–179.

Идея цифровой валюты является довольно новой, и центральные банки по всему миру все еще в полной мере не пришли к единому пониманию регулирования отношений, связанных с цифровыми деньгами, не осознают последствий внедрения такой технологии. Блокчейн, биткойн и другие инновации в секторе финансовых технологий показывают, что они могут улучшить статус-кво, а также продвинуть концепцию цифровой валюты, делая ее реальным

претендентом на замену бумажных денег. Это ставит правительства мира в затруднительное положение, вынуждая своевременно реагировать на изменения финансовой жизни путем признания виртуальной валюты на законодательном уровне.

При этом, если государство оперативно не отреагирует на запросы общества, то это может привести к следующим сложностям:

- отсутствие четкого правового статуса криптовалюты

может послужить причиной того, что цифровые деньги станут средством отмывания денежных средств;

- использование криптовалюты может служить механизмом уклонения от налогов;
- появление множества преступных схем использования криптовалюты вследствие анонимного ее использования¹.

Правительства разных государств совершенно по-разному отреагировали на внедрение цифровых денег в своих странах. Реакция варьировалась от опасений и страха до полного принятия.

Федеральное правительство США еще не заявило о своем праве исключительно регулировать криптовалюты, предоставив отдельным штатам право определять, как их граждане могут участвовать. На данный момент Нью-Йорк, Аризона, Мэн, Невада, Вермонт и другие представили законопроекты в сенаты своих штатов, в основном касающиеся допустимого использования реестров блокчейна и смарт-контрактов для ведения учета и других задач.

Единственные конкретные заявления о криптовалюте, сделанные федеральными органами, касаются того, как люди должны сообщать о своей прибыли и как криптовалюта облагается налогом.

В Европе существует более сложное правовое регулирование криптовалюты. Внутри валютного союза из 19 стран блокчейн идеально подходит для новых правил, требующих прозрачности информации и обмена данными между

рынками и учреждениями, и быстро становится крупнейшим сектором стартапов в регионе.

Поскольку исполнительная власть Европейского парламента в настоящее время создает децентрализованную бухгалтерскую книгу для своих собственных целей, новую группу наблюдения, предназначенную для отслеживания текущих событий, теперь каждая страна может самостоятельно решать вопросы регулирования криптовалюты.

Швейцария решила использовать криптовалюту таким же ненормативным образом, как и многие другие европейские страны. Швейцарский федеральный совет заявил, что, хотя в настоящее время нет необходимости регулировать криптовалюту, законы о том, как финансовый сектор будет использовать их, разрабатываются для определения их статуса как ценных бумаг и налогообложения. Соответственно, в Швейцарии находится быстро развивающаяся сцена стартапов блокчейнов, управляемая инклюзивными общественными организациями, такими как Crypto Valley Association, некоммерческой организацией, призванной стандартизировать внедрение новой технологии блокчейн в швейцарскую экосистему.

В Германии биткойн считается «расчетной единицей», и граждане страны могут торговать ею по своему усмотрению. Однако он также облагается налогом и должен включать НДС при торговле в евро.

¹ Русанова П. А., Лошкарев А. В. Правовое регулирование криптовалюты в России //

Международный журнал гуманитарных и естественных наук. 2020. № 10-4 (49). С. 53.

Германия является еще одним ярким примером того, как правительства избегают путаницы нормативных вопросов, не называя криптовалюту «настоящей» валютой.

В странах Азии взгляд на криптовалюты охватывает весь спектр правового регулирования. Япония, возможно, является самой позитивной страной с точки зрения криптовалюты, и ей удалось стать таковой, признав монеты, такие как биткойн, «законным средством платежа», но не традиционной валютой. Соответственно, банки не могут предлагать своим клиентам биткойны, но и хранить биткойны не является незаконным. Результат был блестящим: многие компании интегрируют платежи в биткойнах в свои услуги и производные контракты, такие как «биткойн-облигация».

Другие государства Азии не могут похвастаться таким прогрессом, со страхом наблюдая за наступлением криптовалюты. В азиатских странах, таких как Бангладеш, Непал и Кыргызстан, использование или торговля виртуальными валютами является незаконной и влечет за собой суровые наказания.

Австралия достигла выгодного баланса в том, как она регулирует технологию криптовалюты. Как и многие другие страны, Австралия не ввела никаких мер, которые потребовали бы интенсивных инвестиций и контроля. Вместо этого

они назвали криптовалюту обычными «деньгами», чтобы иметь возможность облагать налогом тех, кто с ним работает. Так, многие государственные структуры Австралии используют в своей деятельности расчеты с использованием систем блокчейн-технологий.

В 2014 году Центральный Банк России в своем обзоре отметил, что криптовалюта не признается в Российской Федерации как средство платежа, а носит характер денежного суррогата. Также было указано, что использование криптовалюты на территории России приравнивается к финансированию терроризма, а обмен виртуальных денежных средств на рубли и вовсе расценивается как отмывание денежных средств, а все операции с цифровой валютой носят спекулятивный характер².

Далее по результатам такого заявления Центробанка Министерство финансов РФ разместило на официальном портале правовой информации РФ проект закона, центральным положением которого было введение административной и уголовной ответственности за финансовые операции, производимые с помощью цифровой валюты. Однако, Государственная Дума несколько раз отклоняла предложенный законопроект, что не позволило изолировать Россию от мировой цифровизации денежных ресурсов.

² Nikitin K. The legal status of cryptocurrency in Russia // Эж-Юрист. 2017. № 45. URL: https://vegaslex.ru/upload/iblock/fb1/%D0%9D%D0%B8%D0%BA%D0%B8%D1%82%D0%B8%D0%BD%20eng_%D1%8D%D0%B6-

%D0%AE%D1%80%D0%B8%D1%81%D1%82_The%20legal%20status%20of%20cryptocurrency%20in%20Russia.pdf (дата обращения: 03.05.2021).

Также в 2015 году в нижнюю палату Парламента РФ был представлен для рассмотрения законопроект, который предусматривал новую законодательную конструкцию в Кодекс Российской Федерации об административных правонарушениях. Согласно такому законопроекту № 957581-6³, в КоАП РФ планировалось дать легальное толкование денежного суррогата, к которому причислялись и электронные средства платежа, а также установить административную ответственность за использование таких платежных средств. Законопроект не вызвал одобрения у парламентариев и был отклонен в первом чтении.

Далее законодательную инициативу по вопросу урегулирования правового статуса криптовалюты в России взяла на себя Федеральная налоговая служба РФ. В октябре 2016 года ФНС РФ на официальном сайте разместила письмо, в котором было указано на то, что отсутствие законодательного регулирования, а также норм-дефиниций в РФ таких понятий, как «криптовалюта», «денежный суррогат» и «виртуальная валюта» затрудняет правовое регулирование операций, производимых с помощью

приведенных предполагаемых средств платежа в силу того, что отсутствие ясного правового положения цифровых денег в правовом поле РФ не позволяет органам налоговой службы оперативно отслеживать и проверять законность производимых операций на предмет соответствия данных операций налоговому законодательству РФ. ФНС РФ внесла законопроект, предполагающий поправки к федеральному закону № 173-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»⁴. Законопроект был призван урегулировать вопрос субъектов контроля рынка цифровой валюты. Однако, законопроект также не встретил одобрения.

Можно констатировать, что до 2017 года Российская Федерация шла по пути полнейшего отрицания криптовалюты, не предпринимая попыток легализации виртуальной валюты в правовом поле нашей страны⁵.

Тем не менее, Президент РФ в своем указе от 9 мая 2017 г. «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»⁶ определил вектор развития всей цифровой экономики

³ Проект Федерального закона № 957581-6 «Кодекс Российской Федерации об административных правонарушениях» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=139890#0326973589401316%204> (дата обращения: 04.05.2021).

⁴ Проект федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации» // Министерство финансов РФ: официальный

сайт. URL: [https://minfin.gov.ru/m/document/?id_4=23139-](https://minfin.gov.ru/m/document/?id_4=23139-proekt_federalnogo_zakona_o_vnesenii_izmenenii_v_otdelnye_zakonodatelnye_akty_rossiiskoi_federatsii)

[proekt_federalnogo_zakona_o_vnesenii_izmenenii_v_otdelnye_zakonodatelnye_akty_rossiiskoi_federatsii](https://minfin.gov.ru/m/document/?id_4=23139-proekt_federalnogo_zakona_o_vnesenii_izmenenii_v_otdelnye_zakonodatelnye_akty_rossiiskoi_federatsii) (дата обращения: 03.05.2021).

⁵ Полякова В. В., Токун В. Л. Становление рынка цифровых финансовых активов в Российской Федерации // Вестник университета. 2019. № 6. С. 151.

⁶ О Стратегии развития информационного общества в Российской Федерации на 2017–

нашей страны. Президент указал на необходимость в цифровой валюте для России.

С этого момента началась активная работа над законопроектами, которые определяли бы правовое положение виртуальных денег на территории России, признавая их платежным средством.

С точки зрения гражданского права основополагающее значение имеет федеральный закон № 34-ФЗ⁷. Данная законодательная новелла закрепила в статье 144.1 ГК РФ неизвестное российскому праву понятие «цифровые права». Можно заключить, что итогом принятия данного федерального закона является признание цифровых прав объектом гражданских прав⁸.

Важно отметить, что приведенный ранее федеральный закон оставляет дискуссионным вопрос отнесения цифровых прав к перечню объектов гражданского права ввиду того, что не дает толкования понятия «цифровые деньги», к которым относят различные виды «виртуальных» валют⁹.

В связи с названной проблематикой, отсутствует

единообразие судебной практики по делам, связанным с операциями с применением цифровой валюты.

В ходе рассмотрения дела о банкротстве Арбитражный суд не удовлетворил ходатайство финансового управляющего, требующего включения в конкурсную массу должника содержимого криптокошелька. Обоснование такого отказа заключалось в том, что положение криптовалюты в российском законодательстве не урегулировано, а следовательно, ее применение не может быть обеспечено с помощью принудительной силы государства¹⁰.

Однако, можно встретить полярную точку зрения суда на этот счет. Судья, в ходе производства по делу № А40-124668/2017¹¹, приравнял криптовалюту к основной конкурсной массе, указывая на то, что криптовалюта имеет статус электронных денежных средств.

Так, исходя из анализа судебной практики, можно сделать вывод о том, на данный момент дела, связанные с обращением цифровой валюты, разрешаются на основе судейского усмотрения.

2030 годы: указ Президента РФ от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

⁷ О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации: федеральный закон от 18.03.2019 № 34-ФЗ // Собрание законодательства Российской Федерации. 2019. № 12. Ст. 1224.

⁸ Рахимов Э. Х., Морин А. В. К вопросу о правовом регулировании цифровых финансовых активов // Вестник Уфимского юридического института МВД России. 2019. № 3. С. 137.

⁹ Овчинников А. И., Фатхи В. И. Цифровые права как объекты гражданских прав // Философия права. 2019. № 3. С. 104–106.

¹⁰ Решение Арбитражного суда города Москвы по делу № А40-124668/17-71-160 Ф от 5 марта 2018 г. // Картотека арбитражных дел. URL: http://kad.arbitr.ru/PdfDocument/45c24bb9-9d22-4b57-8742-9a778f041b99/A40-124668-2017_20180305_opredelenie.pdf (дата обращения: 03.05.2021).

¹¹ Решение Арбитражного суда Вологодской области от 24 октября 2017 г. по делу № А40-124668/2017 // СудАкт. URL: <https://sudact.ru/arbitral/doc/20EHFIeHovUP/> (дата обращения: 02.05.2021).

Таким образом, Федеральный закон «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации»¹², на наш взгляд нуждается в доработке для возможности его использования в судебной практике.

Важнейшим документом для регулирования правового статуса криптовалюты в РФ является подготовленный уже в 2018 году, но принятый лишь 24 июля 2020 года Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»¹³. Данный документ содержит ряд принципиально новых для российского права положений, призванных решить проблемы определения правового статуса криптовалюты на территории нашей страны, однако, он вступил в силу и подлежит применению лишь с 1 января 2021 года.

К основным и наиболее важным с точки зрения урегулирования положения цифровой валюты в правовом пространстве РФ относятся следующие положения:

- финансовые организации, которые производят операции с цифровыми финансовыми активами, обязаны быть зарегистрированы в едином реестре Банка России;

- цифровые финансовые активы имеют статус объектов гражданского права, в отношении которых возможны сделки купли-продажи, займа и т. д.;

- данные активы можно обменивать между собой;

- приобретение цифровой валюты может производиться через иностранные биржи;

- цифровые финансы могут выступать на территории РФ платежным средством, однако, с их помощью не может производиться оплата товаров и услуг в силу того, что криптовалюта по национальному законодательству не является государственной денежной единицей России;

- уставный капитал финансовых организаций и блокчейн-платформ, осуществляющих транзакции с цифровыми активами, не может составлять менее 50 млн руб.

Таким образом можно говорить о том, что правовое регулирование сферы цифровой валюты только начинает зарождаться. Разработка нормативно-правовых актов, регулирующих правовое положение криптовалюты и блокчейн-технологий, чрезвычайно важна для развития и расширения цифрового

¹² О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации: федеральный закон от 18.03.2019 № 34-ФЗ // Собрание законодательства Российской Федерации. 2019. № 12. Ст. 1224.

¹³ О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 31 июля 2020 г. № 259-ФЗ // Собрание законодательства Российской Федерации. 2020. № 31 (часть I). Ст. 5018.

экономического пространства на территории нашей страны¹⁴.

При этом следует понимать, что множество документов нуждаются в доработке, ряд вопросов остаются неурегулированными:

- Кто должен быть субъектом контроля за цифровыми деньгами?
- Как определяется владелец цифровых активов?
- Какие права имеет владелец криптовалюты, в чем состоят его права и обязанности?
- Можно ли обменивать криптовалюту на деньги и иные объекты гражданских прав?
- Подлежат ли в полной мере применению нормы налогового

законодательства к операциям с криптовалютой?

На наш взгляд, основным субъектом контроля цифровых валют в РФ должен стать Центральный Банк РФ. Также именно этот орган должен гарантировать и обеспечивать цифровые деньги. На Центробанк должны быть возложены полномочия по аккумулированию информации произведенных транзакций по выпуску и обращению криптовалюты, который бы позволял отменить или отследить незаконную операцию.

В связи с этим требуется кардинальный пересмотр его функций и внесение соответствующих положений в ФЗ РФ «О Центральном банке Российской Федерации».

Список литературы

1. Букина С. Е. Правовое регулирование криптовалютной отрасли в России и за рубежом / С. Е. Букина, Паламарчук А. Р. // Проблемы экономики и юридической практики. 2018. № 6. С. 86–92.
2. Овчинников А. И. Цифровые права как объекты гражданских прав / А. И. Овчинников, В. И. Фатхи // Философия права. 2019. № 3. С. 104–112.
3. Полякова В. В. Становление рынка цифровых финансовых активов в Российской Федерации / В. В. Полякова, В. Л. Токун // Вестник университета. 2019. № 6. С. 150–153.
4. Рахимов Э. Х. К вопросу о правовом регулировании цифровых финансовых активов / Э. Х. Рахимов, А. В. Морин // Вестник Уфимского юридического института МВД России. 2019. № 3. С. 134–137.
5. Русанова П. А. Правовое регулирование криптовалюты в России / П. А. Русанова, А. В. Лошкарёв // Международный журнал гуманитарных и естественных наук. 2020. № 10-4 (49). С. 52–56.

¹⁴ Букина С. Е, Паламарчук А. Р. Правовое регулирование криптовалютной отрасли в России и за рубежом // Проблемы экономики

и юридической практики. 2018. № 6. С. 90–92.

Valeria V. Melentieva

Student,

Northern (Arctic) Federal University named after M. V. Lomonosov

(Arkhangelsk, Russian Federation)

melentiewa.valeria@yandex.ru

Scientific supervisor – S. E. Zhura, PhD (Economics), acting Head of the Department of Financial Law and Jurisprudence, Associate Professor of the Department of Financial Law and Jurisprudence

**DEVELOPMENT OF LEGAL REGULATION OF CRYPTOCURRENCY:
EXPERIENCE OF RUSSIA AND FOREIGN COUNTRIES**

Abstract: The article is devoted to the analysis of the legal status of cryptocurrency in Russia and foreign countries: USA, Germany, Switzerland, Japan, Australia. It points to the polarity in the views of state authorities regarding the legalization of the use of digital financial assets. The positions of the courts of the Russian Federation in relation to virtual currency were considered, it was found that cases related to the use of digital money are currently resolved on the basis of judicial discretion.

Keywords: cryptocurrency, blockchain technology, digital financial assets, legal regulation, virtual currency, means of payment, digital rights.

Шандарович Игорь Олегович

Студент,
Белорусский государственный университет
(г. Минск, Республика Беларусь)
Igor.shdanrovich@yandex.by

Кислицкая Надежда Александровна

Студент,
Белорусский государственный университет
(г. Минск, Республика Беларусь)
n.kislickaya@gmail.com

Научный руководитель – А. М. Хлус, кандидат юридических наук, доцент
кафедры криминалистики

**ИДЕНТИФИКАЦИЯ БИТКОИН-АДРЕСОВ И ПОДОЗРЕВАЕМЫХ,
ИЗЪЯТИЕ БИТКОИНОВ С КОШЕЛЬКОВ ПОДОЗРЕВАЕМЫХ**

Аннотация: В данной статье предлагаются способы идентификации биткоин-адресов и подозреваемых, а также пути изъятия биткоинов с кошельков подозреваемых при расследовании преступлений, связанных с хищением биткоинов. Статья содержит информацию о программах, разработанных специально для работы с блокчейном и биткоин-транзакциями, которые повысят эффективность следователя при раскрытии вышеуказанных преступлений.

Ключевые слова: биткоин, преступление, хищение, криптовалюта, идентификация, изъятие, кошелек.

Для цитирования:

Шандарович И. О. Идентификация биткоин-адресов и подозреваемых, изъятие биткоинов с кошельков подозреваемых / И. О. Шандарович, Н. А. Кислицкая // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 180–186.

Как правило, при расследовании преступлений, связанных с биткоином, есть 2 основные цели: идентифицировать подозреваемого и конфисковать биткоины, приобретённые преступным путём.

Криптовалюта, если она используется в «серых» операциях, оставляет много следов в сети.

Однако, идентификация не является чем-то, что может быть отсортировано самим блокчейном. Анонимный характер блокчейна поддерживает только биткоин-адреса без каких-либо ссылок на реальные личности. Поэтому для отслеживания транзакции в блокчейне необходимо объединить информацию,

полученную из блокчейна, с данными, полученными из других источников.

Walletexplorer.com является оптимальным бесплатным инструментом, который связывает биткоин-адреса с известными субъектами включая обменники, майнинговый пул, игровые сайты, кошельки или даркнет. Он был разработан в 2014 году чешским программистом Алесом Яндой.

Разработчик веб-сайта в настоящее время работает в Chainalysis и больше не обновляет Walletexplorer. Тем не менее, веб-сайт продолжает анализировать (обрабатывать) блокчейн, поэтому последние данные по-прежнему доступны, возможно, с небольшой задержкой, что позволяет обрабатывать самые последние входящие данные.

Проводник Walletexplorer прост в использовании и результаты легко интерпретировать. Он работает как поисковая система для биткоин-адресов; когда биткоин-адрес может быть связан с известным объектом, указывается имя объекта. Программа работает с кошельками, а не с адресами, и по этим причинам результаты более информативны и их легче интерпретировать.

Использовать Walletexplorer можно в качестве бесплатного блокчейн-обозревателя, но при просмотре транзакций следует учитывать ложные срабатывания. По этой причине лучше использовать Walletexplorer вместе с blockchain.info, который является источником более

надежной информации, в то время как Walletexplorer дополняет информацию к тому, что обнаружено через blockchain.info.

В отличие от тех преступлений, где злоумышленники хранят деньги в банках (на счетах или в ячейках) или наличными в тайниках, биткоины имеют свою специфику. Кто-то может предположить, что биткоины хранятся на компьютере подозреваемого, однако, мы говорим о том, что биткоины хранятся в блокчейне, который находится на тысячах компьютеров по всему миру.

При этом, на компьютере подозреваемого располагается кошелек, содержащий закрытый ключ, который позволит правоохранителям изъять биткоины с компьютера, если на то будут основания.

Помимо компьютера, закрытый ключ может храниться на другом носителе, например, флешке, телефоне, записан на листке бумаги и т. д. Также он может храниться у третьей стороны, распоряжающаяся биткоинами, или на виртуальной бирже, которая позволяет совершать транзакции при помощи биткоина, не скачивая клиент, или у онлайн-провайдера кошелька¹.

Помимо закрытых ключей, наиболее очевидные результаты, которые обнаружит следователь на ПК преступника – баланс, список входящих и исходящих транзакций и биткоин-адреса, контролируемые кошельком. Тем не менее, при более тщательном рассмотрении можно найти более подробные сведения.

¹ Приватный ключ кошелька Биткоин: где хранится и как узнать // Tehnoobzor. URL: <https://tehnobzor.com/cryptolife/bitcoin/2501->

[privatnyy-klyuch-koshelka-bitkoin-gde-hranitsya-i-kak-uznat.html](https://tehnobzor.com/cryptolife/bitcoin/2501-privatnyy-klyuch-koshelka-bitkoin-gde-hranitsya-i-kak-uznat.html) (дата обращения: 29.04.2021).

IP-адреса узлов, к которым подключен клиент, можно найти в стандартном клиенте Bitcoin Core (Окно->Консоль->Пирь на обоих кошельках – Windows и Mac). Во вкладке «Окно» также содержатся информация о директории блоков и директории данных на этом конкретном компьютере.

При проверке кошелька подозреваемого, удаленный нод с самым ранним временем соединения может дать следователю информацию о том, как долго был открыт кошелек подозреваемого.

По нашему мнению, исследование данных в реальном времени должно осуществляться во всех расследованиях, связанных с виртуальными валютами, однако ограничения ресурсов могут заставить следователей расставить приоритеты. Исследование актуальных данных в реальном времени зависит от характера дела: биткоинов, хранящихся в кошельке, наличия квалифицированного персонала и ресурсов, и вероятности положительного результата.

Очевидно, что особое внимание следует уделять исходящим транзакциям и их временным отметкам. Если есть отметка о недавней исходящей транзакции, следует в первую очередь исследовать RAM (оперативную память компьютера). Большинство кошельков зашифрованы, поэтому требуется пароль для разблокировки закрытого ключа для совершения транзакции. Поэтому, если подозреваемый совершил недавно транзакцию, вполне вероятно, что пароль все еще сохраняется в RAM.

Поскольку в настоящее время нет способа обойти защиту паролем, извлечение пароля из оперативной памяти значительно увеличивает вероятность изъятия биткоинов.

Как уже указывалось выше, существует различное количество кошельков, которые позволяют проверять баланс на своих биткоин-адресах без скачивания всего блокчейна, так называемые «лёгкие кошельки». Самые популярные – Bitcoin Core и Electrum. Данные кошельки скачивают лишь ту часть блокчейна, которая релевантна для пользователя.

Программное обеспечение биткоин-кошельков хранит файл bitcoin-wallet.1 на локальном диске. В этом файле закрытый ключ может быть как в незашифрованном виде, так и зашифрованном. В первом случае доступ к компьютеру подозреваемого – это все, что необходимо для обнаружения биткоина и его перемещения на биткоин-кошелек, подконтрольный правоохранительными органами. Однако, подавляющее большинство пользователей независимо от того, используют ли они биткоин в законных или незаконных целях, шифруют свои биткоин-кошельки.

«Лёгкие» кошельки не загружают блокчейн и, следовательно, не имеют возможности проверять транзакции для сети. Это экономит десятки гигабайт на жестких дисках и вычислительные мощности компьютера. Так, например, Bitcoin Core на персональном компьютере автора скачал лишь 2 Гб блокчейна из 450. По этой причине «легкие» кошельки особенно популярны на

мобильных устройствах и смартфонах, которые ограничены дисковым пространством, вычислительными мощностями и батареями. Поскольку блокчейн постепенно увеличивается, всё большее число пользователей переходит от полных к «лёгким» клиентам (онлайн-кошелькам), или мобильным кошелькам, таким как Coinbase, Blockchain.info или Trust.

Легче всего понять различие между полной нодой и «лёгким» кошельком проводя аналогию с туристом в незнакомом месте. В первом случае у туриста есть телефон, на котором при помощи GPS можно отследить своё местоположение и проложить маршрут на карте до нужного места, а во втором случае у туриста телефона нет и его действия зависят от того, у кого есть карта.

Если следовательно идентифицирует биткоин-адреса подозреваемого в блокчейне, то необходимо учитывать, что невозможно изъять биткоины удаленно (если только подозреваемый держит свои средства на онлайн-бирже). Чтобы изъять биткоины с компьютера подозреваемого, следовательно должен найти:

1. биткоин-кошелек на жестком диске подозреваемого – в этом случае необходим пароль, чтобы осуществлять какие-либо действия с биткоинами, поскольку подавляющее большинство биткоин-кошельков в настоящее время зашифровано;

2. закрытый ключ подозреваемого – в этом случае необходимо импортировать его в биткоин-кошелек;

3. seed-пароль зашифрованного кошелька (как указано в кошельке, это десять ли более случайных символов или восемь и более слов). Seed – специальная кодовая фраза, которая используется для доступа к кошельку².

Изъять биткоины – это не значит просто взять и скопировать файл bitcoin-wallet, импортировать закрытый ключ или ввести seed для работы с программным обеспечением, используемым правоохранными органами. Действуя так, следовательно просто обнаружит соответствующие открытые ключи вместе с суммой неизрасходованных биткоинов. В этом случае, биткоины нельзя считать изъятными, так как сам подозреваемый или другое лицо, у которого есть закрытый ключ, может переместить денежные средства на другой адрес. Чтобы действительно изъять биткоины требуется дополнительный шаг для завершения перевода средств. Таким образом, следовательно должен переместить их на биткоин-адрес, созданный специально для этих целей правоохранными органами.

Здесь следует отметить, что Уголовно-процессуальный кодекс Республики Беларусь не регламентирует порядок и процесс изъятия криптовалюты³.

² Восстановление доступа к кошельку и адресам Bitcoin – мнемоническая seed фраза // Форум сайта Bits.media. URL: <https://forum.bits.media/index.php?/topic/125636-восстановление-доступа-к-кошельку-и->

адресам-bitcoin-мнемоническая-seed-фраза/ (дата обращения: 30.04.2021).

³ Уголовно-процессуальный кодекс Республики Беларусь: Кодекс Республики Беларусь от 24.06.1999 № 295-З: в ред. от

Безопасный кошелек, как правило, должен иметь загруженный блокчейн и быть проверен сообществом, поэтому биткоин-кошелек Bitcoin Core – крайне предпочтительный вариант. Очевидно, официальный биткоин-адрес правоохранительного органа должен быть заранее известен сотрудникам, проводящим обыск или изъятие. Он может быть на бумаге или USB-ключе, чтобы сотрудники могли перемещать биткоины без каких-либо задержек.

Зашифрованный кошелек можно открыть и проверить его баланс, вывести список транзакций и существующие биткоин-адреса. Однако для извлечения закрытого ключа или перевода средств на другой биткоин-адрес потребуется пароль.

Самый очевидный вариант – убедить подозреваемого сотрудничать со следствием. Пароль можно вводить неограниченное количество раз, кошелек не будет заблокирован или удалён. Иными словами, у подозреваемого не будет возможности манипулировать сотрудниками для сокрытия улик.

Можно попытаться взломать пароль при помощи программы `btrecover` с GitHub⁴. Однако, учитывая огромную вариативность паролей и осведомлённость пользователей о простейшей IT-безопасности и важности сложного пароля (особенно, когда речь идёт о

десятках или сотнях тысяч долларов) её использование и шанс на успех можно описать фразой «пальцем в небо».

Третий способ получить необходимые данные – `walletrecoveryservices.com`⁵. Проблема использования данного способа заключается в том, что программа платная. Стандартная цена за услуги – 20 % от стоимости биткоинов на кошельке. Если стоимость содержимого превышает 100 000 \$, то цена падает до 15 %. Цену необходимо заплатить лишь в случае успешного взлома.

Независимо от того, удалось ли изъять биткоины или нет, следователь может извлечь список всех биткоин-адресов, которые были сохранены в биткоин-кошельке подозреваемого. Команда `listaddressgroupings`, введённая через вкладку «Консоль», может использоваться, чтобы просмотреть все биткоин-адреса вместе с потраченными или неизрасходованными средствами. Важно получить этот список, чтобы все биткоин-адреса можно было позже проверить, используя бесплатные или платные программы отслеживания транзакций.

Таким образом, в последнее время криптовалюты получают все более широкое распространение. Однако большинство операций с криптовалютами осуществляется вне правового регулирования Республики

14.04.2021 // ИПС «ЭТАЛОН». Законодательство Республики Беларусь / Нац.центр правовой информ. Республики Беларусь. URL: https://etalonline.by/document/?regnum=hk9900295&q_id=3294668 (дата обращения: 30.04.2021).

⁴ `Btrecover` // GitHub. URL: <https://github.com/gurnec/btrecover> (дата обращения: 30.04.2021).

⁵ Wallet recovery service // Wallet recovery service: official site. URL: <https://www.walletrecoveryservices.com> (дата обращения: 30.04.2021).

Беларусь в том числе и потому, что законодательство не соответствует требованиям времени⁶.

Криптовалюты выпускаются неограниченным кругом анонимных субъектов и все чаще выступают в качестве инвестиционного инструмента и инструмента спекулятивной торговли.

Учитывая интересы общества, биткоин не может оставаться валютой

для преступников. Крайне важно, чтобы блокчейн стал тем местом, где преступники не чувствуют себя в безопасности. Вот почему лица, заинтересованные в технологии блокчейна, например, коммерческие организации по типу Chainanalys, должны помочь правоохранительным органам изучить ее.

Список литературы

1. Приватный ключ кошелька Биткоин: где хранится и как узнать // Tehnoobzor. URL: <https://tehnobzor.com/cryptolife/bitcoin/2501-privatnyy-klyuch-koshelka-bitkoin-gde-hranitsya-i-kak-uznat.html> (дата обращения: 29.04.2021).

2. Шандарович И. О. Виртуальная собственность: абстракция или реальность? / И. О. Шандарович, М. С. Рыбалко // Белорусское право во времени и пространстве: сборник тезисов докладов Республиканской научно-теоретической конференции студентов, магистрантов, аспирантов (Минск, 4 декабря 2019 года) / [под ред. И.П. Манкевич]; УО «Белорусский государственный экономический университет». Минск: БГЭУ, 2020. С. 117–118.

Igor O. Shandarovich

Student,

Belarusian State University
(Minsk, Republic of Belarus)
Igor.shdanrovich@yandex.by

Nadezhda A. Kislitskaya

Student,

Belarusian State University
(Minsk, Republic of Belarus)
n.kislickaya@gmail.com

Scientific supervisor – A. M. Hlus, PhD (Law), Associate Professor of the Department of Criminalistics

⁶ Шандарович И. О., Рыбалко М. С. Виртуальная собственность: абстракция или реальность // Белорусское право во времени и пространстве: сборник тезисов докладов Республиканской научно-теоретической конференции студентов, магистрантов,

аспирантов (Минск, 4 декабря 2019 года) / [под ред. И.П. Манкевич]; УО «Белорусский государственный экономический университет». Минск: БГЭУ, 2020. С. 117–118.

IDENTIFICATION OF BITCOIN ADDRESSES AND SUSPECTED, WITHDRAWAL OF BITCOINS FROM SUSPECTED WALLETS

Abstract: This article offers ways to identify bitcoin addresses and suspects, as well as ways to withdraw bitcoins from the wallets of suspects in the investigation of crimes related to theft of bitcoins. The article contains information about programs designed specifically to work with blockchain and bitcoin transactions, which will increase the efficiency of the investigator in solving the above crimes.

Keywords: bitcoin, crime, theft, cryptocurrency, identification, withdrawal, wallet.

Раздел IV

ГЕНОМНЫЕ ИССЛЕДОВАНИЯ, РЕПРОДУКТИВНЫЕ ТЕХНОЛОГИИ

Кручинина Надежда Валентиновна

Доктор юридических наук, профессор, профессор кафедры криминалистики,
Московский государственный юридический университет
имени О. Е. Кутафина (МГЮА)
(г. Москва, Российская Федерация)
kriminalistmsal@list.ru

**РОЛЬ НАУКИ В ЗАЩИТЕ ОТ КРИМИНАЛЬНЫХ РИСКОВ
ВСПОМОГАТЕЛЬНЫХ РЕПРОДУКТИВНЫХ ТЕХНОЛОГИЙ***

Аннотация: В статье анализируются различные точки зрения на репродуктивные права человека. Обосновывается необходимость защиты репродуктивного здоровья. Использование вспомогательных репродуктивных технологий в России увеличивается. Законодательство, регулирующее правоотношения в данной сфере, нуждается в совершенствовании. Определена роль науки в этом процессе.

Ключевые слова: репродуктивные права человека, репродуктивное здоровье, медицинские услуги, лечение бесплодия, экстракорпоральное оплодотворение, торговля людьми, расследование преступлений.

Для цитирования:

Кручинина Н. В. Роль науки в защите от криминальных рисков вспомогательных репродуктивных технологий // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 188–191.

Организация Объединенных Наций в 1989 году рекомендовала объявить 11 июля Всемирным днем народонаселения. Это еще раз подтверждает важность проблем, связанных с воспроизводством населения, с репродуктивными правами человека для существования и развития любого государства и всей цивилизации в целом.

Репродуктивная функция человека является важной для существования и развития любого государства. Реализация данной

функции предполагает правовое регулирование прав и обязанностей.

Правом на использование достижений вспомогательных репродуктивных технологий (далее – ВРТ) пополнился перечень репродуктивных прав человека, к которым ученые причисляют право решать вопросы о количестве детей, о времени их рождения, право на репродуктивное здоровье.

К вспомогательным репродуктивным технологиям относятся: экстракорпоральное

* Исследование произведено при финансовой поддержке РФФИ рамках научного проекта № 18-29-14084.

оплодотворение (ЭКО), искусственная инсеминация, донорство эмбрионов, ооцитов, спермы, хетчинг (рассечение оболочки эмбриона), внутриплазменная инъекция спермы (ИКСИ, ИМСИ), получение сперматозоидов для ИКСИ, криоконсервация эмбрионов, гамет, перенос эмбрионов, суррогатное материнство, биопсия эмбриона и преимплантационная диагностика.

Использовать перечисленные возможности могут люди не во всех странах. И даже там, где эти технологии разрешены, имеются ограничения, связанные с возрастом, наличием или отсутствием заболеваний; определенные процедуры позволены только одиноким женщинам, но не позволены одиноким мужчинам, разрешены только супружеским парам; существует разная степень свободы при принятии решения о судьбе ребенка, рожденного суррогатной матерью; по-разному решается вопрос об оплате.

В некоторых странах разницу в требованиях к ВРТ медицинские учреждения используют в своих интересах. Например, в северной части острова Кипр, где находится оккупированный Турцией анклав, при использовании вспомогательных репродуктивных технологий предоставляется возможность выбрать пол ребенка¹. Поэтому многие супружеские пары из европейских стран отправляются на север Кипра, где позволяется

родителям выбрать пол своего ребенка при использовании ВРТ.

С вопросами использования возможностей ВРТ связаны проблемы редактирования эмбриона человека, сопряженные с рисками не только медицинского, но также этического и правового характера. Следует отметить, что существует большой разброс мнений относительно применения на практике генетических технологий в отношении человека – от абсолютного отрицания до полной поддержки. Опыт, проведенный китайским ученым Хэ Цзянькуем, который отредактировал геном эмбриона человека и добился рождения первых в мире генетически модифицированных детей, до сих пор обсуждается в научных кругах. Многие ученые критически отнеслись к эксперименту китайского ученого. При обсуждении такого важного вопроса, как редактирование эмбриона человека, ученые отмечают, что существует риск того, что попытки исправить генетический код неродившегося ребенка может принести больше вреда, чем пользы. Среди ученых есть предложения по введению глобального моратория на редактирование эмбриона человека.

На наш взгляд, необходима выработка международных стандартов использования ВРТ.

Прежде всего, обратимся к понятию «стандарт». «Стандарт (от англ. standard – норма-образец), в широком смысле слова – образец, эталон, модель, принимаемые за исходные для сопоставления с ними

¹ Kefalas A. Chypre, l'île où on peut choisir le sexe de son futur bébé // Le Figaro. 2019. 2 juil. P. 16.

подобных объектов. Стандарт как нормативно-технический документ устанавливает комплекс норм, правил, требований к объекту стандартизации. Стандарт может быть разработан как на материальные предметы (продукцию, эталоны, образцы веществ), так и на нормы, правила, требования в различных областях»².

На основе созданных учеными международных стандартов в сфере использования ВРТ необходимо принять международно-правовые документы, направленные на защиту от криминальных рисков ВРТ, а также организовать на постоянной основе на национальном и международном уровнях работу по научному прогнозированию возможного использования достижений науки и техники в преступных целях, для предупреждения этих деяний. Важно создать организацию, осуществляющую мониторинг по реализации международных стандартов в сфере использования ВРТ.

Усилия научного международного сообщества необходимы в деле защиты от криминальных рисков ВРТ. От научного мирового сообщества сейчас многое зависит.

Отсутствие должного правового регулирования в сфере использования ВРТ, международного научного

контроля провоцирует на совершение преступлений в этой сфере³.

Так, в конце июня 2020 года Следственный комитет РФ, возбудил уголовное дело, в отношении учредителей компании, предоставляющих медицинские услуги, связанные с ВРТ, решив, что их действия подпадают под состав статьи 127.1. УК РФ (Торговля людьми). По данным следствия, в квартире жилого дома были найдены пятеро новорожденных младенцев; дети были рождены россиянками для граждан Китая, куда их не смогли переправить из-за закрытия границ⁴.

Для устранения конфликтов и криминального использования в области использования вспомогательных репродуктивных технологий, конечно, важно совершенствование законодательства, регулирующего эту сферу. Высокий уровень злоупотреблений, в том числе преступного характера, в сфере использования ВРТ добавляет аргументов противникам использования этих технологий, которые стремятся ограничить, а иногда и запретить их полностью, что пагубно может сказаться на развитии науки. Важная роль в защите ВРТ от необдуманных нападков отводится науке.

Наука криминалистика также должна внести свой вклад в процесс защиты ВРТ, который, в основном,

² Стандарт // Большой энциклопедический словарь. 2000. Режим доступа: Словари и энциклопедии на сайте Academic.ru. URL: <https://dic.academic.ru/dic.nsf/enc3p/280258#sel=5> (дата обращения: 15.05.2021).

³ Кручинина Н. В. Юридическая ответственность за злоупотребления и преступления в сфере искусственной

репродукции человека // LEX Russica. 2019. № 6 (151). С. 48–51.

⁴ Сидорова Э. СК раскрыл подробности дела о торговле детьми, по которому задержали восемь человек // Life.ru. URL: <https://life.ru/p/1334828> (дата обращения: 15.05.2021).

заключается в выработке мер по предупреждению преступлений в этой сфере, создании методик расследования преступлений, совершаемых в этой области,

выработке эффективных технических, тактических и методических рекомендаций по проверке значимой с криминалистических позиций информации.

Список литературы

1. Кручинина Н. В. Расследование преступлений против семьи: монография / Н. В. Кручинина, Н. Д. Пятибратова; под общ. ред. Е. П. Ищенко. М. : Проспект, 2019. 131 с.
2. Кручинина Н. В. Юридическая ответственность за злоупотребления и преступления в сфере искусственной репродукции человека // LEX Russica. 2019. № 6 (151). С. 48–51.
3. Стандарт // Большой энциклопедический словарь. 2000. Режим доступа: Словари и энциклопедии на сайте Academic.ru. URL: <https://dic.academic.ru/dic.nsf/enc3p/280258#sel=5>.
4. Kefalas A. Chypre, l'île ou on peut choisir le sexe de son future bèbè // Le Figaro. 2019. 2 juil. P. 16.

Nadezda V. Kruchinina

Doctor of law, professor, professor of department of criminalistics,
Kutafin Moscow State Law University (MSAL)
(Moscow, Russian Federation)
kriminalistmsal@list.ru

THE ROLE OF THE SCIENCE IN PROTECTING ASSISTED REPRODUCTIVE TECHNOLOGIES FROM CRIMINAL RISKS

Abstract: In the article the different points of view on human rights of reproduction are analyzed. It justifies the need to protect reproductive health. The number of cases of the use of assisted reproductive technologies in Russia is increasing every year. Legislation governing legal relations in this area needs further development. The role of the science in this process is determined.

Keywords: reproductive rights, reproductive health, medical services, infertility treatment, in vitro fertilization, human trafficking, crime investigation.

Бородин Сергей Сергеевич

Кандидат юридических наук, доцент кафедры гражданского и
предпринимательского права,
Самарский национальный исследовательский университет
имени академика С. П. Королева
(г. Самара, Российская Федерация)
borodinss@lenta.ru

**РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ ПО ИСПОЛЬЗОВАНИЮ
РЕЗУЛЬТАТОВ ГЕНЕТИЧЕСКИХ ИССЛЕДОВАНИЙ ПРИ
СОГЛАСОВАНИИ УСЛОВИЙ ДОГОВОРОВ***

Аннотация: В статье указывается, что генетические персональные данные обладают самостоятельной хозяйственной ценностью, поскольку являются источником коммерчески востребованной информацией. При этом использование результатов генетических исследований создает значимые риски для отдельных людей и общества в целом, в связи с возможностью дискриминационных решений на основании генетических данных конкретного индивидуума. Особо подчеркивается, что в основном риски дискриминации связаны с созданием общих генетических профилей. Обращается отдельное внимание на то, что в любых случаях, в которых имеет место автоматизация, должны быть предусмотрены приемлемые меры защиты прав, свобод и законных интересов субъекта данных, включая права на оспаривание решения.

Ключевые слова: результаты генетических исследований, циркадианные гены, персональные данные, договорное право, дискриминация.

Для цитирования:

Бородин С. С. Регулирование отношений по использованию результатов генетических исследований при согласовании условий договоров // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 192–197.

Использование современных технологий позволяет оптимизировать условия для наиболее эффективного осуществления экономического оборота. В том числе в настоящее время перспективными

направлениями является внедрение машиночитаемого права¹, использование смарт-контрактов, применения нейронных сетей. Генетические технологии, включая результаты исследований

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-14073.

¹ См.: Вашкевич А. М. Автоматизация права: право как электричество. М.: Симплоер, 2019. С. 13.

циркадианных генов, позволяют не только осуществить тонкую настройку отношений в сфере медицинского обслуживания, но также собранные в результате генетические персональные данные приобретают самостоятельную ценность в качестве практически незаменимого источника коммерчески востребованной информации, поскольку позволяют сформулировать предложения товаров и услуг, обладающие повышенной ценностью для потенциального клиента в связи с учетом его привычек и потребностей. Таким образом, персональные генетические данные обладают тройственным значением, поскольку являются исходными данными для осуществления дальнейших фундаментальных научных исследований, решения прикладных вопросов профилактики и лечения конкретного пациента, а также используются участниками гражданского оборота.

В аспекте фундаментальных научных исследований, на международном уровне в 1996 году учеными были разработаны «Бермудские принципы», предусматривающие, в том числе, что все данные о последовательностях ДНК должны опубликовываться в течение двадцати четырех часов после их появления, что сформировало современную практику открытого доступа и концепцию отношения к соответствующей информации как к

всеобщему источнику знаний². В дальнейшем указанный подход получил развитие в Концепции ответственного обмена геномными данными и данными, связанными со здоровьем человека, разработанной под руководством Глобального Альянса в сфере геномики и здравоохранения³. Цель указанной Концепции, в том числе заключается в обеспечении эффективного и ответственного обмена геномными данными.

Осуществление генетических исследований поддерживается и на государственном уровне. Так, согласно плану мероприятий («дорожной карте») «Развитие биотехнологий и геной инженерии» на 2018–2020 годы», утвержденному Распоряжением Правительства РФ от 28.02.2018 № 337-р, для инновационного развития современной экономики одним из ключевых направлений направления развития технологий являются биотехнологии. Согласно плану мероприятий («дорожной карте») по совершенствованию законодательства и устранению административных барьеров в целях обеспечения реализации Национальной технологической инициативы по направлению «Хелснет», утвержденному распоряжением Правительства РФ от 05.05.2018 № 870-р, предполагается устранение основных ограничений в области нормативного правового

² See: Frizzo-Barker J., Chow-White P. From Patients to Petabytes: Genomic Big Data, Privacy, and Informational Risk // Canadian Journal of Communication. 2014. Vol. 39, № 4. P. 615–625.

³ See: Global Alliance for Genomics and Health. URL: <https://www.ga4gh.org/wp-content/uploads/Framework-Russian-translation.pdf> (accessed: 16.05.2021).

регулирования, препятствующих развитию организаций, функционирующих на территории РФ в рамках рынка «Хелснет», и их выходу на международные рынки, путем совершенствования законодательства РФ, в том числе урегулирования порядка проведения доклинических и клинических исследований, генетической диагностики нового поколения, включая внедрение механизма лабораторно-разработанных диагностических тестов.

Однако, с другой стороны, использование результатов генетических исследований создает определенные риски для отдельных людей и общества в целом, в том числе, в части этнической и иной дискриминации. В связи с этим, Всеобщей декларацией о геноме человека и правах человека (принята 11 ноября 1997 г. на 29 сессии Генеральной конференции ООН по образованию, науке и культуре – ЮНЕСКО) провозглашено, что личность человека не может сводиться к его генетическим характеристикам, и требует уважения его уникальности и неповторимости (ст. 2), при этом дополнительно оговаривается, что по признаку генетических характеристик никто не может подвергаться дискриминации, недопустимо посягательство на права человека, основные свободы и человеческое достоинство (ст. 6). Кроме того, в соответствии со ст. 16 Конвенции о защите прав человека и человеческого достоинства в связи с применением достижений биологии и медицины от 04.04.1997 исследования на людях могут осуществляться только в

ситуациях, когда нет других, альтернативных, методов исследования, которые были бы сравнимы по эффективности, а проект планируемых изысканий прошел утверждение уполномоченным органом по итогам осуществления независимой экспертизы научной обоснованности выполнения такого исследования.

Также особый статус генетических данных человека отмечается и в ст. 4 Международной декларации о генетических данных человека (принята резолюцией Генеральной конференции ЮНЕСКО по докладу Комиссии III на 20-м пленарном заседании 16 октября 2003 года), где закреплено, что они не только могут указывать на проявления генетической предрасположенности соответствующего лица; но и содержать информацию, роль и значение которой во время сбора биологических образцов может быть неизвестно, и в связи с этим отдельно подчеркивается требование о конфиденциальном характере генетических данных человека, соответствующем уровню защиты этих данных и биологических образцов. Запрет дискриминации дополнительно закреплен в ст. 7 указанной декларации, в которой подчеркивается, что генетические данные человека не должны использоваться для дискриминации и нарушения права и свободы человека, включая стигматизацию того или иного лица, семьи или группы.

В России легальное определение понятия геномной информации содержится в п. 3 ст. 1 Федерального закона от 03.12.2008 № 242-ФЗ «О

государственной геномной регистрации в Российской Федерации», согласно которой она представляют собой персональные данные, включающие кодированную информацию об определенных фрагментах дезоксирибонуклеиновой кислоты физического лица или неопознанного трупа, не характеризующих их физиологические особенности. При этом предусматривается обязательная и добровольная государственная геномная регистрация. Указанным федеральным законом прямо предусматривается, что условия получения, учета, хранения, использования, передачи и уничтожения биологического материала и обработки геномной информации при проведении государственной геномной регистрации должны исключать возможность их утраты, повреждения, искажения, несанкционированных доступа к ним и их передачи.

Вместе с тем, необходимо дополнительно обратить внимание на то, что, как отмечается в литературе, риски дискриминации связаны не столько с возможностью необоснованного разглашения персональных данных, сколько с созданием общих генетических профилей, которые впоследствии применяются при принятии решений, включая несправедливое или дискриминирующее поведение. В свою очередь, для формирования таких профилей не требуется повторная идентификация человека, поскольку вполне достаточно

анонимных, но агрегированных данных, обработанных с использованием методов машинного обучения и интеллектуального анализа данных. В связи с этим для нивелирования указанных рисков необходима разработка и внедрение новых методов обеспечения конфиденциальности. Отметим, что уже выработаны два основных подхода к решению указанной проблемы. Первый путь состоит в запрете дискриминации по признакам, связанным с генетикой. Так, в 2008 году в США был принят Закон о недискриминации генетической информации, направленный против дискриминации со стороны медицинских страховщиков или работодателей, в соответствии с которым медицинским страховщикам запрещено корректировать страховые взносы, запрашивать или требовать прохождения генетического теста, получать и использовать их результаты при принятии решений, а также запрашивать или покупать генетическую информацию для целей андеррайтинга. Одной из проблем указанного подхода является то, что необходимо доказать, что решение принято по дискриминационным основаниям⁴. Второй вариант – исключение автоматизации принятия решения или обеспечение минимального уровня защиты интересов человека при задействовании такого механизма. Например, ст. 22 Регламента Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических

⁴ Sariyar M., Schlünder I. Challenges and Legal Gaps of Genetic Profiling in the Era of Big Data

// Frontiers in Big Data. November. 2019. Vol. 2. Article 40. P. 1–5.

лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС, устанавливает общее правило о том, что человек не должен подпадать под действие решения, основанного исключительно на автоматической обработке, включая формирование профиля, которое порождает юридические последствия в отношении него или существенно воздействует на него. При этом в любом случае, когда имеет место автоматизация, должны быть предусмотрены приемлемые меры защиты прав, свобод и законных интересов субъекта данных, включая, на минимальном уровне: право требования принятия решительных мер со стороны контролера; права на выражение своей точки зрения; право на оспаривание решения. В таком подходе проблемным является определение инструментария, обеспечивающего достаточный уровень защиты интересов человека при принятии автоматических решений на основе, в том числе генетического паспорта, а также

государственных и частных баз генетических данных.

Таким образом, для осуществления комплексного регулирования возможности использования результатов генетических исследований в рамках переговоров о заключении договоров и формирования его условий необходимо использовать междисциплинарный подход, включающий изыскания в сфере юриспруденции, биологии и цифровых технологий, и проработать два основных блока вопросов: обеспечение сохранения анонимности полученных генетических данных при одновременном отслеживании источников; обеспечение устранения рисков дискриминации реципиентов данных и членов их семей. На основе соответствующих теоретических разработок должна быть сформирована нормативная правовая база, закрепляющая всю совокупность возникающих при этом отношений и создающая гарантии соблюдения прав и свобод человека, недопущения недискриминации человека по причинам, связанным с геномом.

Список литературы

1. Вашкевич А. М. Автоматизация права: право как электричество М.: Симплойер, 2019. 256 с.
2. Frizzo-Barker J. From Patients to Petabytes: Genomic Big Data, Privacy, and Informational Risk / J. Frizzo-Barker, P. Chow-White // Canadian Journal of Communication. 2014. Vol. 39, № 4. P. 615–625.
3. Sariyar M. Challenges and Legal Gaps of Genetic Profiling in the Era of Big Data / M. Sariyar, I. Schlünder // Frontiers in Big Data. November. 2019. Vol. 2. Article 40. P. 1–7.

Sergey S. Borodin

PhD (Law), Associate Professor of the Department of Civil and Entrepreneurial Law,
Samara National Research University
named after Academician S. P. Korolev
(Samara, Russian Federation)
borodinss@lenta.ru

REGULATION OF RELATIONSHIPS ON USING THE RESULTS OF GENETIC STUDIES WHEN CONCLUDING CONTRACTS

Abstract: The article indicates that genetic personal data have an independent economic value, since they are a source of commercially demanded information. At the same time, the use of the results of genetic research creates significant risks for individuals and society as a whole, due to the possibility of discriminatory decisions based on the genetic data of a particular individual. It is emphasized that the main risks of discrimination are associated with the creation of common genetic profiles. In the article special attention is drawn to the fact that in any cases in which automation takes place, acceptable measures must be provided to protect the rights, freedoms and legitimate interests of the data subject, including the right to challenge the decision.

Keywords: genetic research results, circadian genes, personal data, contract law, discrimination.

Попов Вадим Петрович
Кандидат юридических наук
(г. Москва, Российская Федерация)
popov.vp1993@gmail.com

ФАЛЬСИФИКАЦИЯ ГЕНЕТИЧЕСКИХ МАТЕРИАЛОВ: КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ*

Аннотация: Генетические технологии находят все более широкое распространение в современной жизни. Однако, недостаточное правовое регулирование в данной сфере, низкий уровень понимания специфики проблемы большинством работников правоохранительных органов, недостаточная техническая оснащенность создают почву для совершения фальсификации генетических материалов. Изучение специальной литературы и анализ международного опыта показывают, что сфера искусственной репродукции человека особенно подвержена злоупотреблениям и преступлениям связанным с подлогом ДНК-материалов.

Ключевые слова: криминалистика, предупреждение преступлений, вспомогательные репродуктивные технологии, суррогатное материнство, фальсификация, генетические материалы.

Для цитирования:

Попов В. П. Фальсификация генетических материалов: криминалистический аспект // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 198–202.

В соответствии со статей 2 Конвенции о биологическом разнообразии генетический материал представляет собой любой материал растительного, животного, микробного или иного происхождения, содержащий функциональные единицы наследственности¹.

Использование генетического материала – многоаспектная проблема. Представляется

необходимым обратить особое внимание на два направления в данной сфере, которые имеют особое значение для криминалистики: геномная регистрация и защита генетического материала от фальсификации.

Проблема получения максимально полной справочной информации об индивидуальных признаках человека и расширения криминалистической регистрации

* Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 18-29-14084.

¹ СЗ РФ. 1996. № 19. Ст. 2254.

является актуальной как для ученых-криминалистов, так и для практически работников². Однако, разработанные меры, нацеленные на оптимизацию расследования и на предупреждение преступлений, на практике не всегда выполняются, что вызывает опасения.

В рамках увеличения возможностей криминалистической регистрации был принят Федеральный закон от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации»³. В пункте «ж» ст. 9 этого Закона установлено, что обязательной государственной дактилоскопической регистрации подлежат граждане Российской Федерации, иностранные граждане и лица без гражданства, подозреваемые в совершении преступления, обвиняемые в совершении преступления, осужденные за совершение преступления, подвергнутые административному аресту.

Позднее в связи с достижениями в области биотехнологий был принят Федеральный закон от 03.12.2008 № 242-ФЗ «О государственной геномной регистрации в Российской Федерации»⁴. Согласно п. 1 ч. 1 ст. 7 данного Закона обязательной государственной геномной

регистрации подлежат лица, осужденные и отбывающие наказание в виде лишения свободы за совершение тяжких или особо тяжких преступлений, а также всех категорий преступлений против половой неприкосновенности и половой свободы личности.

На практике зачастую не выполняются требования указанных законов о дактилоскопическом и генетическом учетах⁵.

Примечателен следующий случай. Решением Заводского районного суда г. Кемерово удовлетворен иск прокурора г. Кемерово в интересах Российской Федерации к ФКУ ИК-22 ГУФСИН по Кемеровской области об устранении нарушения законодательства о государственной геномной регистрации, выразившегося в бездействии администрации по исполнению требования закона, обязывающего изымать (отбирать) биологические образцы у лиц, отбывающих наказание в виде лишения свободы, в целях получения геномной информации. Судом установлено, что в исправительной колонии в 2016 г. не прошли процедуру геномной регистрации более 90 % лиц, подлежащих

² Самищенко С. С. Современная дактилоскопия: основы и тенденции развития. М., 2004. 456 с.; Жога Е. Ю., Васенин А. Ю., Варченко И. А. Роль государственной геномной регистрации в предупреждении, раскрытии и расследовании преступлений // Гуманитарные, социально-экономические и общественные науки. 2017. № 6-7. С. 117–121; Михайлов М. А. Международная научно-практическая конференция в Государственной Думе «Совершенствование

системы дактилоскопической экспертизы» // Библиотека криминалиста. Научный журнал. 2016. № 1 (24). С. 368–378.

³ СЗ РФ. 1998. № 48. Ст. 3806.

⁴ СЗ РФ. 2008. № 49. Ст. 5740.

⁵ Кручинина Н. В. Проверка достоверности информации о личности преступника средствами дактилоскопии // Сборник Международной научно-практической конференции «Совершенствование системы дактилоскопической экспертизы». М., 2016. С. 45.

обязательному генетическому учету, часть осужденных были освобождены. Административным ответчиком решение было обжаловано со ссылкой на невозможность исполнения требований закона *вследствие ненадлежащего материально-технического обеспечения*, однако апелляционным судом решение оставлено без изменения⁶.

Неисполнение нормативных правовых актов провоцирует на совершение фальсификаций, а пренебрежительное отношение к рекомендациям криминалистики весьма негативно влияет на расследование преступлений.

Понимая огромное положительное криминалистическое значение расширения дактилоскопической и геномной регистрации, не следует забывать, что вероятность неправомерного использования геномной информации лица также возрастает. Наиболее опасной формой неправомерного использования генетической информации является фальсификация генетического материала, биологических следов на месте происшествия.

Серьезную озабоченность вызывает возможность

злоумышленника фальсифицировать ДНК-доказательства на месте преступления, подменив образцы крови, слюны, содержащие ДНК человека⁷.

Указанная проблема является актуальной во всех развитых странах. В Израиле биохимики неоднократно обращали внимание на теоретическую и практическую возможность подделать образец ДНК человека, используя информацию из генетического профиля, при этом образцы биологического материала, содержащие ДНК, не требуются.

Несмотря на то, что выявить такую фальсификацию сейчас практически невозможно, разработки в этом направлении ведутся отдельными организациями. Например, фирма Nucleix занимается специальным оборудованием, предназначенным для выявления амплификации (копирования) в образцах ДНК⁸.

А. Г. Блинов и М. М. Лапунин в работе «Пределы вмешательства уголовного права в сферу исследования генома человека» приводят уникальный пример, который должен заставить задуматься всех криминалистов, занимающихся проблемой генетических

⁶ Калиниченко П. А. Развитие судебной практики по делам в сфере геномики человека: мировой опыт и Россия // Lex russica. 2019. № 6. С. 30–36.

⁷ Pollack A. DNA Evidence Can Be Fabricated, Scientists Show // N. Y. Times. 2009. 17 aug. URL: <http://www.nytimes.com/2009/08/18/science/18dna.html>, archivedat (accessed: 01.05.2021); Богданова Е. Е. Правовые проблемы и риски генетической революции: генетическая информация и дискриминация // Lex russica. 2019. № 6. С. 18–29.

⁸ Блинов А. Г., Лапунин М. М. Пределы вмешательства уголовного права в сферу исследования генома человека // Вестник Пермского университета. Юридические науки. 2020. № 50. С. 810; Authentication of forensic DNA samples / D. Frumkin, A. Wasserstrom, A. Davidson, A. Grafit // Forensic Science International: Genetics. 2010. Vol. 4, Issue 2. P. 95–103. DOI: 10.1016/j.fsigen.2009.06.009.

исследований. Житель Невады Крис Лонг сделал операцию по пересадке костного мозга. Донором являлся гражданин Германии. Судебный медик из США взял пробы Криса Лонга до и после операции. Анализ ДНК Лонга после операции поразил ученых, так как сперматозоиды Лонга несли в себе исключительно генетический материал донора из ФРГ⁹. Очевидно, что потенциальные дети Лонга генетически будут детьми гражданина Германии; если Лонг совершит преступление, то осуществить его идентификацию по генетическим материалам будет невозможно.

Представляется, что важной предупредительной (превентивной) мерой в борьбе с совершением новых преступлений, серьезным

инструментом, используемым для эффективного расследования совершенных преступлений, является расширение возможностей по работе с генетическим материалом.

Однако, развитие генетических технологий влечет возникновение новых угроз и вызовов. Фальсификация генетического материала, представляет опасность для обеспечения безопасности искусственной репродукции человека, нормального функционирования общественных отношений, направленных на защиту основополагающих естественных прав, может являться как самостоятельным способом совершения преступлений, так и способом противодействия расследованию.

Список литературы

1. Блинов А. Г. Пределы вмешательства уголовного права в сферу исследования генома человека / А. Г. Блинов, М. М. Лапунин // Вестник Пермского университета. Юридические науки. 2020. № 50. С. 804–831.
2. Богданова Е. Е. Правовые проблемы и риски генетической революции: генетическая информация и дискриминация // Lex russica. 2019. № 6. С. 18–29.
3. Жога Е. Ю. Роль государственной геномной регистрации в предупреждении, раскрытии и расследовании преступлений / Е. Ю. Жога, А. Ю. Васенин, И. А. Варченко // Гуманитарные, социально-экономические и общественные науки. 2017. № 6-7. С. 117–121.
4. Калиниченко П. А. Развитие судебной практики по делам в сфере геномики человека: мировой опыт и Россия // Lex russica. 2019. № 6. С. 30–36.
5. Authentication of forensic DNA samples / D. Frumkin, A. Wasserstrom, A. Davidson, A. Grafit // Forensic Science International: Genetics. 2010. Vol. 4, Issue 2. P. 95–103. DOI: 10.1016/j.fsigen.2009.06.009.

⁹ Блинов А. Г., Лапунин М. М. Пределы вмешательства уголовного права в сферу исследования генома человека // Вестник Пермского университета. Юридические науки. 2020. № 50. С. 810; Murphy H. When a

DNA Test Says You're a Younger Man, Who Lives 5,000 Miles Away // N. Y. Times. 2019. 7 dec. URL: <https://www.nytimes.com/2019/12/07/us/dna-bone-marrow-transplant-crime-lab.html> (accessed: 01.05.2021).

6. Murphy H. When a DNA Test Says You're a Younger Man, Who Lives 5,000 Miles Away // N. Y. Times. 2019. 7 dec. URL: <https://www.nytimes.com/2019/12/07/us/dna-bone-marrow-transplant-crime-lab.html>.
7. Pollack A. DNA Evidence Can Be Fabricated, Scientists Show // N. Y. Times. 2009. 17 aug. URL: <http://www.nytimes.com/2009/08/18/science/18dna.html>, archived at.

Vadim P. Popov
PhD (Law)
(Moscow, Russian Federation)
popov.vp1993@gmail.com

FALSIFICATION OF GENETIC MATERIALS: FORENSIC ASPECT

Abstract: Genetic technologies are becoming more widespread in modern life. However, insufficient legal regulation in this area, a low level of understanding of the specifics of the problem by the majority of law enforcement officials, and insufficient technical equipment create grounds for falsifying genetic materials. The research of special literature and the analysis of international experience show that the field of artificial human reproduction is especially susceptible to abuse and crimes associated with forgery of DNA materials.

Keywords: criminalistics, crime prevention, assisted reproductive technology, surrogate motherhood, falsification, genetic material.

УДК 349

Юдин Егор Витальевич

Младший научный сотрудник, аспирант,
Санкт-Петербургский государственный университет
(г. Санкт-Петербург, Российская Федерация)
yudinegorv@gmail.com

СОЦИАЛЬНАЯ ЗНАЧИМОСТЬ ГЕНЕТИЧЕСКИХ ТЕХНОЛОГИЙ И ИХ ИСПОЛЬЗОВАНИЯ В МЕДИЦИНСКИХ ЦЕЛЯХ: ВЫЗОВ СУЩЕСТВУЮЩЕМУ ОТЕЧЕСТВЕННОМУ ПРАВОВОМУ РЕГУЛИРОВАНИЮ*

Аннотация: В статье рассматриваются генетические технологии и их использование в процессе оказания медицинской помощи. Автором предлагается определение генетических технологий, выявляется сфера их использования в медицинских целях, а также эксплицируется их социальная природа и значимость. Делается вывод об отсутствии системного правового регулирования генетических технологий и их использования в медицинских целях, а также вывод о необходимости учёта их социальной сущности и значимости.

Ключевые слова: генетические технологии, социальная значимость, медицинская помощь, геномика, геномная медицина, социальный риск, правовое регулирование.

Для цитирования:

Юдин Е. В. Социальная значимость генетических технологий и их использования в медицинских целях: вызов существующему отечественному правовому регулированию // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 203–209.

На сегодняшний день происходит процесс активного внедрения новых медицинских и биомедицинских явлений, преобразующих и переосмысливающих биосоциальную ткань общественных отношений, в практику оказания медицинской помощи пациентам.

Так, не вызывающим сомнение фактом стали новые биомедицинские

инновационные технологии, позволяющие говорить о развитии геномной медицины и так называемой 4П-медицины (прогностической, профилактической, персонифицированной, партнёрской). Расшифровка генетического материала, редактирование генома человека (в том числе с использованием технологии CRISPR/Cas9), модификация

* Настоящая работа подготовлена в рамках поддержанного РФФИ научного проекта № 20-311-90051.

зародышевой линии клеток, активное внедрение методов клеточной и тканевой инженерии, геномики, транскриптомики, протеомики, метаболомики, а также применение биомедицинских клеточных продуктов в процессе оказания медицинской помощи изменяют биосоциальную действительность и позволяют по-новому взглянуть как на существо медицинской помощи и место пациента при её оказании в отдельности, так и на правоотношения в сфере современной медицины в целом. К новым биомедицинским инновационным технологиям относятся в том числе и генетические технологии.

Социальная природа и значимость генетических технологий детерминирует необходимость обеспечения оптимального юридического воздействия (выработки механизмов правового регулирования) на новые объективные процессы, возникающие в сфере использования генетических технологий.

Генетические технологии чрезвычайно разнообразны по своей природе, в связи с чем и сфера их использования на сегодняшний день также очень широка и находится в

состоянии перманентного расширения. Учитывая отсутствие законодательно закреплённой дефиниции генетических технологий и не умаляя эвристической ценности предложенных различными авторами своих определений¹, в рамках настоящего исследования мы под *генетическими технологиями будем понимать совокупность методик, инструментов, методов, процессов и тестов, которые разрабатываются на основе знаний о геноме*².

В апреле 2019 г. Россия приступила к реализации Федеральной научно-технической программы развития генетических технологий на 2019–2027 годы (далее – Программа)³. В мае 2020 г. на совещании о развитии генетических технологий в России Президент В. В. Путин объявил о создании в рамках национального проекта «Наука» трёх геномных центров мирового уровня⁴. В июне 2020 г. Президент В. В. Путин поручил Правительству России создать информационно-аналитическую систему хранения и обработки генетических данных «Национальная база генетической информации»⁵.

Указанное также является еще одним фактом, свидетельствующем о

¹ Мохов А. А. Генетические технологии: понятие, сущность, виды // Генетические технологии и право в период становления биоэкономики / отв. ред. А. А. Мохов, О. В. Сушкова. М.: Проспект, 2020. С. 92–96.

² The Evolution of Public Health Genomics: Exploring Its Past, Present, and Future / C.M. Molster, F.L. Bowman, G.A. Bilkey, [et al.] // Frontiers in Public Health. 2018. Vol. 6. P. 1–3.

³ Об утверждении Федеральной научно-технической программы развития генетических технологий на 2019–2027

годы: постановление Правительства РФ от 22.04.2019 г. № 479 // СПС «КонсультантПлюс».

⁴ Путин заявил о создании трех геномных центров // Российская газета. 2020. 14 мая. URL: <https://rg.ru/2020/05/14/putin-zaiavil-o-sozdanii-treh-genomnyh-centrov.html> (дата обращения: 01.05.2021).

⁵ Перечень поручений по итогам совещания по вопросам развития генетических технологий (утв. Президентом РФ 04.06.2020 г. № Пр-920) // СПС «КонсультантПлюс».

необходимости анализа и формирования наиболее совершенного нормативного правового ландшафта в сфере генетических технологий. Более того, с учётом специфики генетических технологий и высокого рискованного их характера для человека и общества, с целью формирования отвечающих сегодняшним реалиям правовых механизмов необходимо использование риск-ориентированного подхода, который позволяет понять существующие объективные процессы, а затем, исходя из степени риска, ясно определить параметры самого регулирования (в том числе и правового). Важно подчеркнуть и то, что выстраивание механизмов правового регулирования рассматриваемых общественных отношений должно осуществляться с учётом необходимости соблюдения баланса интересов трех сторон:

1. представителей

медицинского и научного сообщества, заинтересованных в перманентном развитии новых биотехнологий (включая генетических) и научного знания;

2. лиц, в отношении которых подобные технологии применяются в процессе оказания медицинской помощи;

3. остальных граждан, стремящихся поддерживать состояние своего здоровья на должном уровне, и общества в целом.

Одним из направлений реализации вышеобозначенной

Программы является развитие генетических технологий в медицине, основные разделы которого связаны с проведением работ по:

- биоинформатическому анализу генетических структур, которые обуславливают возникновение патологических процессов, разработке редакторов и систем доставки, которые способствуют избирательному активированию, модифицированию или выключению целевых генов-мишеней для задач, решаемых с использованием технологий геномного редактирования;

- созданию моделей заболеваний с использованием лабораторных животных или культур клеток;

- противодействию инфекциям, в том числе ретровирусным, при которых происходит встраивание вирусного генетического материала в геном человека;

- редактированию генетических вариантов и дефектов генома, которые приводят к заболеваниям с описанной генетической этиологией;

- модификации клеток, в том числе иммунной системы, при мультигенных и других патологиях⁶.

Также в Программе закреплено, что проведение работ по переходу к персонализированной медицине *позволит обеспечить*, среди прочего, *нормативно-правовое сопровождение применения генетических технологий в биомедицине*.

⁶ Об утверждении Федеральной научно-технической программы развития генетических технологий на 2019-2027 годы:

постановление Правительства РФ от 22.04.2019 г. № 479 // СПС «КонсультантПлюс».

В соответствии с действующим российским законодательством медицинская помощь с использованием генетических технологий является специализированной, в том числе высокотехнологичной, медицинской помощью⁷, к которой относятся, например:

- медико-генетическое консультирование⁸,
- пренатальная диагностика⁹,
- неонатальный скрининг¹⁰,
- преимплантационное генетическое тестирование¹¹,
- генотерапия¹²,
- молекулярно-генетические исследования для выявления предрасположенности к генетически детерминированным заболеваниям, диагностики (генодиагностика) и лечения заболеваний¹³ и т. д.

Более того, согласно утвержденным в 2020 году клиническим рекомендациям по

заболеванию проксимальная спинальная мышечная атрофия 5q (СМА) основным способом диагностики данного заболевания является проведение молекулярно-генетического исследования мутаций в гене SMN1 всем пациентам с подозрением на СМА 5q с целью выявления делеции экзонов 7 или 7-8 и молекулярно-генетического подтверждения диагноза¹⁴; исходя из положений клинических рекомендаций по заболеванию дифференцированный рак щитовидной железы в рамках иных диагностических исследований для дифференциальной диагностики опухолей щитовидной железы рекомендуется проводить молекулярно-генетическое исследование мутаций в гене BRAF и

⁷ Об основах охраны здоровья граждан в Российской Федерации: федеральный закон Российской Федерации от 21.11.2011 г. № 323-ФЗ // СПС «КонсультантПлюс».

⁸ О порядке использования вспомогательных репродуктивных технологий, противопоказаниях и ограничениях к их применению: приказ Минздрава России от 31.07.2020 г. № 803н // СПС «КонсультантПлюс».

⁹ О порядке использования вспомогательных репродуктивных технологий, противопоказаниях и ограничениях к их применению: приказ Минздрава России от 31.07.2020 г. № 803н // СПС «КонсультантПлюс».

¹⁰ О массовом обследовании новорожденных детей на наследственные заболевания: приказ Минздравсоцразвития РФ от 22.03.2006 г. № 185 // СПС «КонсультантПлюс».

¹¹ О порядке использования вспомогательных репродуктивных технологий, противопоказаниях и ограничениях к их применению: приказ Минздрава России от 31.07.2020 г. № 803н // СПС «КонсультантПлюс».

¹² О государственном регулировании в области генно-инженерной деятельности: федеральный закон от 05.07.1996 г. № 86-ФЗ // СПС «КонсультантПлюс».

¹³ О государственном регулировании в области генно-инженерной деятельности: федеральный закон от 05.07.1996 г. № 86-ФЗ // СПС «КонсультантПлюс».

¹⁴ Клинические рекомендации «Проксимальная спинальная мышечная атрофия 5q» (утв. Министерством здравоохранения РФ, 2020 г.) // Рубрикатор клинических рекомендаций Минздрава РФ. URL: <http://cr.rosminzdrav.ru/#!/schema/1018> (дата обращения: 10.05.2021).

иных мутаций (RAS, RET/PTC, PAX8/PPAR-γ, TERT и т. д.)¹⁵

Вышеприведённое свидетельствует об имплицитно заложенной социальной сущности и высокой социальной значимости использования генетических технологий в процессе оказания медицинской помощи с целью профилактики, диагностики и лечения различных заболеваний и состояний, включая моногенные и полигенные (мультифакториальные) заболевания, что предопределяет необходимость выстраивания эффективных правовых механизмов регулирования рассматриваемых общественных отношений с учётом принципа постоянства социальной защиты участников на всех этапах оказания медицинской помощи с использованием генетических технологий.

При этом, социальная сущность и значимость генетических технологий в медицинской сфере не ограничивается только их применением для профилактики, диагностики и лечения различных заболеваний и состояний обратившихся за медицинской помощью пациентов, а также для реализации пациентами своих прав (например, репродуктивных). Социальная сущность и высокая социальная значимость использования генетических технологий в процессе

оказания медицинской помощи проявляется ещё и в том, что:

1. Развитие генетических технологий в медицинской сфере позволит повысить качество и продолжительность жизни человека, особенно при активном накоплении знаний о генофонде нации (эпидемиология генома человека¹⁶).

2. Активное включение последних достижений науки в сфере геномики в практику оказания медицинской помощи позволит не только выстроить динамичное и необходимое в сегодняшнее время взаимодействие между научным и медицинским сообществом, но и будет способствовать эффективному противодействию различным инфекциям, пандемиям (что сейчас особенно актуально) и снижению потерь от заболеваний.

Анализ существующего российского нормативного правового поля, в той или иной степени регулирующего общественные отношения в сфере использования генетических технологий при оказании медицинской помощи, позволяет говорить, к сожалению, об эклектичности и неоднородности существующих механизмов правового регулирования в рассматриваемой сфере общественных отношений, а также об игнорировании их социальной значимости. Правовые нормы, связанные с генетическими технологиями и их прямым либо

¹⁵ Клинические рекомендации «Дифференцированный рак щитовидной железы» (утв. Министерством здравоохранения РФ, 2020 г.) // Рубрикатор клинических рекомендаций Минздрава РФ.

URL: <http://cr.rosminzdrav.ru/#!/schema/977> (дата обращения: 10.05.2021).

¹⁶ The Evolution of Public Health Genomics: Exploring Its Past, Present, and Future / C.M. Molster, F.L. Bowman, G.A. Bilkey, [et al.] // Frontiers in Public Health. 2018. Vol. 6. P. 1–3.

опосредованным использованием при оказании медицинской помощи, содержатся в различных нормативных правовых актах, между которыми, к сожалению, взаимосвязь прослеживается слабо, что свидетельствует об отсутствии системности в правовом регулировании рассматриваемой сферы общественных отношений.

В качестве одного из подобных примеров выделим текущую ситуацию в законодательстве, в рамках которой Федеральный закон от 05.07.1996 г. № 86-ФЗ «О государственном регулировании в области генно-инженерной деятельности»¹⁷, положения которого в своем абсолютном большинстве связаны с вопросами использования генетических технологий в сельском хозяйстве, промышленности и других подобных областях, упоминает генодиагностику и генотерапию при оказании гражданам медицинской помощи и даже раскрывает дефиниции данных понятий. Между тем, Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны

здоровья граждан в Российской Федерации»¹⁸, будучи главным нормативным правовым актом, регулирующим вопросы оказания медицинской помощи, указанные понятия совсем не упоминает.

Подводя итог, отметим, что для целей системного выстраивания правовых механизмов регулирования генетических технологий и их использования в медицинских целях необходимо принятие отдельного федерального закона, посвящённого генетическим технологиям, который будет отражать эксплицированную в настоящей работе социальную сущность и значимость генетических технологий, их имманентную специфику, единообразный терминологический аппарат и принципы регулирования и т. д. Реализация указанного предложения будет в полной мере соответствовать направлению реализации Программы в части нормативно-правового сопровождения применения генетических технологий в биомедицине.

Список литературы

1. Мохов А. А. Генетические технологии: понятие, сущность, виды // Генетические технологии и право в период становления биоэкономики / отв. ред. А. А. Мохов, О. В. Сушкова. М.: Проспект, 2020. С. 92–105.
2. The Evolution of Public Health Genomics: Exploring Its Past, Present, and Future / C.M. Molster, F.L. Bowman, G.A. Bilkey, [et al.] // Frontiers in Public Health. 2018. Vol. 6. P. 1–11.

¹⁷ О государственном регулировании в области генно-инженерной деятельности: федеральный закон от 05.07.1996 г. № 86-ФЗ // СПС «КонсультантПлюс».

¹⁸ Об основах охраны здоровья граждан в Российской Федерации: федеральный закон Российской Федерации от 21.11.2011 г. № 323-ФЗ // СПС «КонсультантПлюс».

Yegor V. Yudin

Junior research assistant, postgraduate student,
St. Petersburg State University
(Saint Petersburg, Russian Federation)
yudinegorv@gmail.com

**THE SOCIAL SIGNIFICANCE OF GENETIC TECHNOLOGIES AND THEIR
USE FOR MEDICAL PURPOSES: A CHALLENGE TO THE CURRENT
DOMESTIC LEGAL REGULATION**

Abstract: The article discusses genetic technologies and its use in the process of providing medical care. The author offers a definition of genetic technologies, identifies the scope of its use for medical purposes, and explicates its social nature and significance. It is concluded that there is no systematic legal regulation of genetic technologies and their use for medical purposes, as well as the conclusion that it is necessary to take into account its social nature and significance.

Keywords: genetic technologies, social significance, medical care, genomics, genomic medicine, social risk, legal regulation.

Раздел V

ИНТЕРНЕТ, СОЦИАЛЬНЫЕ СЕТИ

Щелконогова Елена Владимировна

Кандидат юридических наук, доцент

кафедры уголовного права,

Уральский государственный юридический университет

(г. Екатеринбург, Российская Федерация)

shelkonogova-ele@mail.ru

УГОЛОВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРАВООТНОШЕНИЙ, ВОЗНИКАЮЩИХ В СЕТИ ИНТЕРНЕТ*

Аннотация: Рост объёмов информации, компьютерных сетей и числа пользователей, упрощение их доступа к циркулирующей по сетям информации существенно повышает вероятность хищения или разрушения этой информации. Наибольшую общественную опасность представляют преступления, связанные с неправомерным доступом к компьютерной информации. Известно, что рассматриваемое правонарушение имеет очень высокую латентность, которая по различным данным составляет 85–90 %. Более того, факты обнаружения незаконного доступа к информационным ресурсам на 90 % носят случайный характер.

Преступление данного вида, как показывает мировая практика, наносит огромный материальный и моральный вред. Так, например, ежегодные потери только делового сектора США от несанкционированного проникновения в информационные базы данных составляют от 150 до 300 млрд долларов.

В современных условиях социально-экономического развития Российской Федерации компьютерная преступность стала реальностью общественной жизни.

Ключевые слова: сеть Интернет, киберпреступность, состав преступления, социальные сети, средство совершения преступления, объект уголовно-правовой охраны, медиаконтроль.

Для цитирования:

Щелконогова Е. В. Уголовно-правовое регулирование правоотношений, возникающих в сети Интернет // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 211–217.

С самого своего появления и дальнейшего развития Интернет стал объектом изучения социальных и гуманитарных наук как особая специфическая реальность, которая

имеет свои закономерности развития и формы существования. Из всех главных достижений в развитии средств массовой коммуникации за последние 20 лет можно назвать

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16001.

всемирную сеть Интернет. Интернет на сегодняшний день относится к пятому этапу технологического развития человечества. Предшествующие четыре этапа – это обработка энергии воды, паровая энергия, электричество и электроника. Сегодня смело можно заявить, что стадия использования Интернета в качестве среды общения достигла своего апогея. Социальные сети, форумы, чаты, сайты по интересам и идеям обязательные элементы жизни современного человека.

По статистике на 2020 год 81 % жителей России являются пользователями Интернета (118 000 000 человек). В среднем люди пользуются Интернетом в день 6 часов 55 минут. Наиболее распространенными сайтами по просмотру видео являются Youtube (23,9 млн чел.), Yandex (22,5 млн чел.), «ВКонтакте» (20,1 млн чел.), «Одноклассники» (11,4 млн чел.). Россияне очень заботятся о приватности своих данных: 60 % пользователей активно интересуются вопросом: «Как большие компании пользуются нашими персональными данными?», 34 % россиян раз в месяц чистят куки. По гендерной принадлежности наиболее распространенными среди женщин являются приложения «ВКонтакте» и «Инстаграм», у мужчин – «ВКонтакте» и «Ютуб». Активных пользователей соцсетей или мессенджеров: 70 000 000 человек (48 % населения). Пользуются для

доступа к соцсетям или мессенджерам смартфоном: 90 % населения¹.

3 ноября 2017 года на закрытии Форума по ответственному развитию искусственного интеллекта была принята Монреальская декларация об ответственном развитии искусственного интеллекта (г. Монреаль, Канада). В ней говорится о том, что искусственный интеллект – это результат глобального технического и научного прогресса, способный приносить значительную пользу обществу. Однако, внедрение ИИ может повлечь за собой ущемление свободы выбора среди отдельных личностей и групп, снижение уровня жизни, нарушение структуры рынков труда².

Сеть Интернет и информация, содержащаяся в ней, могут выступать как объект защиты уголовного права, так и являться средством совершения преступления. Информация, находящаяся в сети Интернет, с точки зрения состава преступления может выступать в качестве различных элементов:

- Как **объект** преступления. Например, в главе «Преступления в сфере компьютерной информации» родовым объектом выступают отношения, обеспечивающие общественную безопасность, видовым объектом – общественные отношения, обеспечивающие безопасный оборот компьютерной информации, а также безопасность критической информационной инфраструктуры РФ (компьютерная безопасность).

¹ Статистика пользователей интернета в России // РусИнд.ру: финансы и статистика. URL: <https://rusind.ru/polzovateli-interneta-v-rossii.html> (дата обращения: 20.04.2021).

² Бегишев И. Р., Хисамова З. И. Искусственный интеллект и уголовный закон: монография. М., 2021. С. 183.

Основным непосредственным объектом конкретных составов преступлений в сфере компьютерной информации могут выступать либо отношения, обеспечивающие безопасный оборот компьютерной информации (ст. 272, 273, 274 УК РФ), либо отношения, обеспечивающие безопасность критической информационной инфраструктуры РФ (ст. 274.1 УК РФ)³.

- Как **предмет** преступления: ст. 140 «Отказ в предоставлении гражданину информации», ст. 155 «Разглашение тайны усыновления (удочерения)», ст. 327 «Подделка, изготовление или оборот поддельных документов».

- Как **средство** совершения преступления: ст. 128.1 «Клевета». В ст. 163 «Вымогательство» распространение позорящих сведений является разновидностью угрозы с целью получения материальной выгоды.

В большом количестве составов *угроза* также является средством совершения преступления. В частности, угроза причинения вреда жизни, здоровью (ст. 119 «Угроза убийством или причинением тяжкого вреда здоровью»), имущественного ущерба (в ст. 205 «Террористический акт» угроза совершения взрыва, поджога также может повлечь причинение имущественного ущерба).

Составы мошенничества, в том числе и с использованием компьютерных технологий, также

можно отнести к системе составов, в совершении которых фигурирует информация. В данном случае информация является средством совершения преступления.

Уголовное право выполняет функцию защиты или охраны какой-либо информации от неправомерного распространения. Например, информация о лицевых счетах и денежных средствах, используемая при совершении хищений. Возможна защита общества от распространения вредоносной информации, как публично (ст. 280 «Публичные призывы к осуществлению экстремистской деятельности»), так и в сети Интернет (распространение вирусов – ст. 273 УК РФ). Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьёзное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям⁴.

³ Уголовное право России. Части Общая и Особенная: учебник / под ред. А.В. Бриллиантова. М., 2021. С. 999.

⁴ Интернет-преступность в России // Википедия – свободная энциклопедия. URL: <https://ru.wikipedia.org/wiki/Интернет->

Лидирующее место статистика компьютерных преступлений отводит России по числу пострадавших от кибератак. В 2019 году ими стали 85 % пользователей, в 2020 выявлено более 11000 киберпреступлений. Около половины из них приходится на мошенничество. В связи со сложностью ведения учета, латентностью данных правонарушений, реальная статистика преступлений в Интернете в несколько раз больше. За последние 5 лет, с ростом рынка электронных платежных систем растет и количество преступлений в области компьютерной информации. Одним из новых видов мошенничества стали кражи из электронных кошельков. Суммы ущерба от компьютерных махинаций и число осужденных по этой статье несоразмерно – в 2020 ущерб составил 1,48 млрд. долларов, а осуждено 126 человек за полгода⁵.

Термины «компьютерная преступность» или «киберпреступность» появились в американской, а затем и в зарубежной литературе в начале 1960-х годов, когда были выявлены первые случаи преступлений, совершенных с использованием ЭВМ. В СССР одно из первых компьютерных преступлений – автоматизированное хищение 78 тыс. рублей, совершенное в Вильнюсе⁶.

В связи с изложенной проблематикой острую актуальность приобретают методы борьбы с данными видами преступлений.

Некоторые исследователи предлагают такой неординарный способ, как медиакритика. Под этим термином они подразумевают область знания в журналистике, деятельность которой направлена на объективную оценку и анализ работы средств массовых коммуникаций. Получившая свое развитие, благодаря социальным сетям и блогам, гражданская медиакритика может стать гарантом объективной оценки деятельности пользователей самими же пользователями.

Контроль интернет-пространства является распространенной практикой во всем мире. Самой жесткой мерой считается блокирование или запрет доступа к сайтам, содержащим информацию, нарушающую действующее в той или иной стране законодательство. Распространена также фильтрация информационного потока в местах общего пользования, при которой в интернет-кафе, в учебных заведениях, на предприятиях принимаются меры для ограничения доступа к информации на основе пополняющихся списков. Фильтрация контента может осуществляться на основе «черных списков» (запрета доступа к адресам, содержащимся в списке), «белых списков» (разрешения доступа только к определенным

преступность_в_России (дата обращения: 19.04.2021).

⁵ Статистика преступлений: данные по странам мира // Vawilon.ru. URL:

<https://vawilon.ru/statistika-prestuplenij/> (дата обращения: 19.04.2021).

⁶ Уголовное право России. Части Общая и Особенная: учебник. С. 998.

адресам), а также по ключевым словам⁷.

В рамках системы МВД создано «Управление К», задачами которого являются:

- борьба с нарушением авторских и смежных прав (ст. 146 УК РФ, ст. 7.12 КоАП РФ);
- выявление незаконного проникновения в компьютерную сеть (ст. 272 УК РФ);
- борьба с распространителями вредоносных программ (ст. 273 УК РФ);
- выявление нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ);
- выявление использования подложных банковских карт (ст. 159 УК РФ);
- борьба с распространением порнографии посредством сети Интернет и компакт-дисков (ст. 242 УК РФ);
- выявление незаконного подключения к телефонным линиям (ст. 165 УК РФ, ст. 13.2 КоАП РФ);
- борьба с незаконным оборотом радиоэлектронных (РЭС) и специальных технических средств (СТС) (ст. 138 УК РФ, ст. 171 УК РФ, ст. 14.1, 14.42 КоАП РФ).

Управление является одним из самых засекреченных подразделений МВД России и входит в состав Бюро специальных технических мероприятий Министерства

внутренних дел Российской Федерации⁸.

Проблема киберпреступности чрезвычайно актуальна в современном мире, необходимо выявить направления правового регулирования Интернет-отношений, чтобы уменьшить количество киберпреступлений:

- Защита личных данных и частной жизни в сети Интернет;
- Регулирование электронной коммерции и иных сделок и обеспечение их безопасности;
- Защита интеллектуальной собственности;
- Борьба против противоправного содержания информации и противоправного поведения в сети Интернет;
- Правовое регулирование электронных сообщений⁹.

Таким образом, роль уголовного права в регулировании возникающих новых общественных отношений, связанных с развитием искусственного интеллекта, все более возрастает. Такое явление как киберпреступность требует от государства решительных мер по противодействию и борьбе с ним. Такая деятельность требует специальной подготовки, поскольку данный вид преступности имеет высокую латентность, также могут возникнуть проблемы с доказыванием

⁷ Жусупова А. М., Сулейменова А. Э. Возможности регулирования отношений в сети Интернет через гражданскую медиакритику. URL: <http://docplayer.ru/84466143-Vozmozhnosti-regulirovaniya-otnosheniy-v-seti-internet-cherez-grazhdanskuyu-mediakritiku.html> (дата обращения: 19.04.2021).

⁸ Управление «К» // Академик. URL: <https://dic.academic.ru/dic.nsf/ruwiki/1589634> (дата обращения: 19.04.2021).

⁹ Методы борьбы с киберпреступностью // Студопедия. URL: https://studopedia.ru/11_139589_metodi-borbi-s-kiberprestupnostyu.html (дата обращения: 19.04.2021).

факта совершения преступления, установлением элементов состава преступления, например, субъекта (который может находиться в любой точке мира), субъективной стороны. С другой стороны, искусственный интеллект несет мощный позитивный заряд, который в сфере уголовного права и правоприменения может выражаться в создании алгоритмов квалификации преступлений, которые будут помогать следователям, судьям правильно вынести решение по

конкретному делу. Даже камеры наружного наблюдения, видеорегистраторы, помогающие собрать ценные доказательства, являются проявлением развития компьютерных технологий в нашей жизни. В связи с чем, дальнейшее развитие компьютерных технологий и искусственного интеллекта представляется важной и необходимой тенденцией развития современного общества.

Список литературы

1. Бегишев И. Р. Искусственный интеллект и уголовный закон: монография / И. Р. Бегишев, З. И. Хисамова. М.: Проспект, 2021. 192 с.
2. Жусупова А. М. Возможности регулирования отношений в сети Интернет через гражданскую медиакритику / А. М. Жусупова, А. Э. Сулейменова. URL: <http://docplayer.ru/84466143-Vozmozhnosti-regulirovaniya-otnosheniy-v-seti-internet-cherez-grazhdanskuyu-mediakritiku.html>.
3. Интернет-преступность в России // Википедия – свободная энциклопедия. URL: https://ru.wikipedia.org/wiki/Интернет-преступность_в_России.
4. Методы борьбы с киберпреступностью // Студопедия. URL: https://studopedia.ru/11_139589_metodi-borbi-s-kiberprestupnostyu.html.
5. Статистика пользователей интернета в России // РусИнд.ру: финансы и статистика. URL: <https://rusind.ru/polzovateli-interneta-v-rossii.html>.
6. Статистика преступлений: данные по странам мира // Vawilon.ru. URL: <https://vawilon.ru/statistika-prestuplenij/>.
7. Уголовное право России. Части Общая и Особенная: учебник / под ред. А.В. Бриллиантова. М.: Проспект, 2021. 1344 с.
8. Управление «К» // Академик. URL: <https://dic.academic.ru/dic.nsf/ruwiki/1589634>.

Elena V. Shchelkonogova
 PhD (Law), Associate Professor of the
 Department of Criminal Law,
 Ural State Law University
 (Yekaterinburg, Russian Federation)
shelkonogova-ele@mail.ru

CRIMINAL REGULATION OF LEGAL RELATIONS ARISING IN THE INTERNET*

Abstract: The growth of the volume of information, computer networks and the number of users, the simplification of their access to information circulating through the networks significantly increases the likelihood of theft or destruction of this information. The greatest public danger is posed by crimes related to illegal access to computer information. It is known that the offense under consideration has a very high latency, which, according to various sources, is 85–90 %. Moreover, the facts of detection of illegal access to information resources are 90 % random.

A crime of this type, as world practice shows, causes enormous material and moral harm. For example, the annual losses of the US business sector alone from unauthorized entry into information databases range from 150 to 300 billion dollars.

In the modern conditions of the socio-economic development of the Russian Federation, computer crime has become a reality in public life.

Keywords: Internet, cybercrime, corpus delicti, social networks, means of committing a crime, object of criminal law protection, media control.

* The reported study was funded by RFBR according to the research project № 18-29-16001.

Очеретько Елена Александровна

Кандидат юридических наук, доцент кафедры гражданского и
предпринимательского права,
Елецкий государственный университет им. И. А. Бунина
(г. Елец, Российская Федерация)
lena.ocheretko@yandex.ru

**ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПУБЛИЧНОГО
ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ, СОЦИАЛЬНЫХ СЕТЕЙ И
МЕДИАРЕСУРСОВ**

Аннотация: В настоящее время Интернет играет важную роль для каждого человека, проникая во все сферы нашей деятельности. Удобство, комфорт, скорость – все эти качества современных коммуникативных связей дают любому гражданину широкие возможности для плодотворной профессиональной деятельности, нахождения на связи с родственниками и друзьями в течение 24 часов, формируют оптимальный поиск необходимой информации, сотрудникам правоохранительных органов – помощь в поимке правонарушителей и раскрытии преступлений, для ученых – в дальнейшей разработке нано-технологий и прочих глобальных процессов; Интернет – вездесущ. Но, в то же время, недостаточное правовое регулирование любых медиаресурсов и социальных сетей, упущенный механизм воздействия на правонарушителей, невозможность скорейшего пресечения распространения определенного рода негативной информации – сводят на нет многие достоинства и возможности Глобальной сети. В данной статье автор расставляет акценты над приоритетами в правовом регулировании отношений в сфере публичного использования сети Интернет и предлагает пути совершенствования данных правоотношений.

Ключевые слова: медиаресурсы, публичное использование сети Интернет, социальные сети, мессенджеры.

Для цитирования:

Очеретько Е. А. Проблемы правового регулирования публичного использования сети Интернет, социальных сетей и медиаресурсов // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 218–223.

Одним из самых негативных примеров недавнего времени пользования Глобальной сетью стал созданный преступником И. Г. Телеграм-канал накануне совершенного им жестокого

преступления – нападения на учеников и учителей школы-гимназии № 175 г. Казани. В своем канале преступник за 20 минут до совершенного им зверского преступления призывал к насилию. По

данным основателя социальной сети «ВКонтакте» и «Телеграм» – Павла Дурова – за 15 минут до осуществления роковых выстрелов И. Г. сделал публичным (общедоступным) свой канал, открыв доступ к своим призывам широкой аудитории. Одним из важных моментов этой страшной трагедии стало то, что сотрудниками правоохранительных органов в течение одного часа данный канал был заблокирован. Полагаем, что подобные процессуальные действия необходимо совершать, как можно скорее, чтобы предотвратить серийность указанных преступлений и не допустить вовлечения в них еще большей аудитории. В то же время, в момент подобных преступлений спасительным для жертв моментом могла бы стать возможность у пострадавших, которые не находятся в поле видимости террористов, обратиться за помощью через мессенджер WhatsApp к родственникам или напрямую в правоохранительные органы. Писать на сайт правоохранительных органов абсолютно нерезультативно, звонить по телефону Службы спасения 112 небезопасно, т. к. можно быть услышанным преступниками. А вот, оказавшись в ситуации похищения, будучи заложником или раненым, гражданин смог бы с великой долей безопасности для себя набрать сообщение в WhatsApp и попросить о помощи.

Считаем своевременным и необходимым внести предложение

для МЧС России о совместных мероприятиях быстрого реагирования на чрезвычайные ситуации с операторами сотовых сетей. В частности, подобное предложение имело место в 2019 г. в Кыргызстане, когда предполагалась интеграция усилий МЧС и WhatsApp через собственное приложение «112 Кыргызстан». Разработчики предполагали, что подобная функция позволит любому пользователю WhatsApp оповестить службу спасения о возникновении чрезвычайного происшествия. Служба сможет по определению геолокации (местоположению) и imei-коду телефона определить местоположение пострадавшего.

Вспомним трагедию в Беслане. Немало времени понадобилось силовикам, чтобы обнаружить террористов, отсутствие связи правоохранительных органов с жертвами преступления – также препятствовало их скорейшему высвобождению.

На своей странице в социальных сетях – ВКонтакте и Instagram названный выше преступник И. Г. в Казани разместил график из 8 школ по порядковым номерам города Казани. И далее было подобное сообщение: «Завтра будет что-то нечто. По всей Казани установлено 36 бомб. Вся Казань будет в крови». Встает закономерный вопрос: почему администраторы данных ресурсов не блокируют подобные публикации?

Если в Likee¹ разместить видео, содержащее призывы к насилию в

¹ Likee (старое название LIKE) – социальная сеть, пользователи которой могут создавать и распространять короткие музыкальные

видеоклипы с нанесением спецэффектов и инструментов дополненной реальности. Приложение разработано сингапурской

статусе «публичное», то велика вероятность, что администрация данной интернет-сети не пропустит это видео, заблокировав его. Каждое видео висит на рассмотрении (в случае, если администратор ресурса, на котором оно размещено, сомневается в его гуманности). Если же формат «приватный», то, велика вероятность размещения данного видео. В случае жалоб пользователей сети данное видео будет заблокировано, либо весь аккаунт.

Трансляция в Likee осуществляется с тем, чтобы пообщаться с блогером. Подобное возможно и в ресурсе Instagram². Если в Likee пользователь нарушает правила трансляции (например, демонстрирует обнаженные тела, органы, наркотики, алкоголь), то администратор ресурса отключает трансляцию (мера разового характера) и блокирует ее на один год (мера длительного характера). Замороженную трансляцию можно обжаловать в администрации социальной сети. Если аккаунт был заблокирован, то даже, если вновь его создать, то владельцу страницы не представится возможным вести трансляцию (live). Пока в Likee нет

определенного уровня (особое количество подписчиков, активность), то также невозможно ее осуществлять. Кроме этого, в аккаунте пользователя-блогера должен быть указан возраст, не менее 16 лет. Однако отмечаются случаи, когда пользователь сам недобросовестно указывает свой возраст.

Также, лицо, ведущее трансляцию, может заблокировать того, кто, например, нецензурно ведет себя, ограничить ему доступ по типу «закрытый профиль». В TikTok³ администрация ресурса может заблокировать аудио- и видеоконтент. На данной платформе можно выложить видео, но оно проходит модерацию (цензуру). К сожалению, в TikTok руководство ресурса может оставить видео с насильственной сценой или убийством. При этом делается пометка «неприемлемый контент». В то же время интерфейс данного ресурса на этом этапе будет отображать две клавиши: 1) пропустить; 2) все равно посмотреть.

Одноклассники – это не просто сеть, которая фактически не подлежит модерации (цензуре), но и еще имеет наибольшую скорость распространения медиаресурсов.

компанией Vigo. Хотя сервис предназначен для пользователей старше 16 лет, значительную долю аудитории составляют дети и подростки от 5 до 12 лет. По количеству лайков на 2020 год первое место в приложении занимают девочки из России // Википедия. URL: <https://ru.wikipedia.org/wiki/Likee> (дата обращения: 17.05.2021).

² Instagram – приложение для обмена фотографиями и видеозаписями с элементами социальной сети, позволяющее снимать фотографии и видео, применять к ним фильтры, а также распространять их

через свой сервис и ряд других социальных сетей // Википедия. URL: <https://ru.wikipedia.org/wiki/Instagram> (дата обращения: 17.05.2021).

³ ТикТок – сервис для создания и просмотра коротких видео, принадлежащий пекинской компании «ByteDance», основанный в 2018 г. в Китае и распространившийся на территорию остальных государств, реализуемый посредством скачиваемых на гаджеты приложений // Википедия. URL: <https://ru.wikipedia.org/wiki/TikTok> (дата обращения: 17.05.2021).

Видеофайлы очень быстро набирают популярность и пересылаются от пользователя к пользователю.

Некоторые социальные сервисы и сети пытаются подавить излишнюю социальную активность. Так, в Instagram пользователю может быть такая активность ограничена (присвоен «бан») за превышение подписчиков в день и лайков (положительных отзывов, отмечаемых символом). С 2021 г. такими основаниями могут послужить: превышение лимитов подписок, комментариев, лайков; одинаковые комментарии под всеми «постами»; демонстрация обнаженного тела, в том числе детей (кормление грудью, шрамы от мастэктомии, изображение голого тела в живописи и скульптуре); экстремизм, противозаконные материалы; одновременный выход с разных устройств (временно может быть заморожена страница). Таким образом, тех правовых мер, которые принимают администраторы интернет-сервисов и социальных сетей, явно недостаточно в борьбе с очень быстрым распространением фото- и видеофайлов, текстов в блогах, всевозможных призывов. И, если, например, выявление материалов экстремистского характера на том или ином сайте или странице в социальной сети ведет к уголовному или административному наказанию соответствующих лиц (ст. 20.29 КоАП РФ, ст. 280 УК РФ), объявлении материалов запрещенными и включению их в соответствующий список экстремистских материалов, то и сами

владелец сетей и медиаресурсов, которые представляют свою платформу для подобного рода деятельности, также обязаны усовершенствовать техническое наполнение своего контента пользователями, не допуская включения в него противозаконных элементов.

Вместе с тем, именно указанные вопросы подлежат более тщательному урегулированию на уровне закона ввиду того, что пользование социальными сетями и мессенджерами осуществляется гражданами круглосуточно. Причем, модернизировать правовое регулирование указанных выше вопросов представляется необходимым в максимально короткие сроки. В качестве действенных мер – предложения блокировать каналы, изымать видео- или фотофайлы, пресекать трансляции.

Параллельно следует отметить, что в отношении размещения в социальных сетях материалов клеветнического характера, порочащих честь, достоинство и деловую репутацию лиц, на данный момент эти вопросы не только достаточно урегулированы законодательством, но и имеется существенная судебная практика. Так, решением Свердловского областного суда было признано незаконным опубликование в сети Интернет видеоматериалов, порочащих честь и достоинство физического лица. В ходе рассмотрения дела было выявлено, что лицом на канале YouTube⁴ было

⁴ YouTube – видеохостинг, предоставляющий пользователям услуги

хранения, доставки и показа видео. YouTube стал популярнейшим видеохостингом и

выложено видео, где автор ролика критиковал человека и демонстрировал публично порочащие сведения о нем. Суд признал данные действия незаконными и обязал выплатить компенсацию потерпевшей в размере 500 тысяч рублей. Указанной меры ответственности можно было бы избежать, либо в случае, если бы потерпевшая дала согласие на размещение информации о ней (что само по себе абсурдно), либо, если бы данная информация не имела порочащего личность человека характера⁵.

С 10 января 2021 года законодательно установлена ответственность за размещение клеветнических материалов в социальных сетях в виде штрафа до 1 млн рублей, а за ложное обвинение в преступлении против половой неприкосновенности и половой свободы – до 5 млн рублей, либо лишение свободы. Объектом выступает честь и достоинство (ст. 152 ГК РФ) одного лица, либо группы лиц. В отношении юридического лица – деловая репутация. Аналогичному наказанию подвергается лицо и за распространение заведомо непроверенной информации. Наказание за клевету в сети Интернет

гораздо жестче, чем в устном публичном виде. Например, высказывание порочащих сведений о человеке в публичных местах наказывается штрафом до 500 рублей, а подобные действия, совершенные в социальных сетях – в размере до 1 млн рублей. Причем, субъектом уголовной ответственности являются исключительно физические лица. Президиум Пленума Верховного Суда РФ в «Обзоре практики ... № 1» (п. 20)⁶ уточнил основания, по которым размещение информации в социальной сети, так называемый «пост» (публикация) выступает основанием для предъявления иска о защите деловой репутации.

Таким образом, становится очевидным, что, поскольку граждане вовлекаются в процесс использования социальных сетей, медиаресурсов и мессенджеров круглосуточно и ежедневно, то следует максимально обезопасить пользователей от негативной информации, особенно касающейся посягательства на честь и доброе имя человека. Важным является и рассмотрение вопроса о возможности обращения граждан за помощью в Службу спасения путем подачи смс-сообщения в WhatsApp на уровне законотворческого процесса.

вторым сайтом в мире по количеству посетителей // Википедия. URL: <https://ru.wikipedia.org/wiki/YouTube> (дата обращения: 17.05.2021).

⁵ Апелляционное определение Свердловского областного суда от 26.09.2018 по делу № 33-16192/2018 // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/cons/cgi/online.cgi?re>

q=doc&base=SOUR&n=172089#043906717915440074 (дата обращения: 17.05.2021).

⁶ Обзор практики рассмотрения судами дел по спорам о защите чести, достоинства и деловой репутации (утв. Президиумом Верховного Суда РФ 16.03.2016 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_195322/ (дата обращения: 15.05.2021).

Elena A. Ocheretko

PhD (Law), Associate Professor of the Department of Civil and Business Law,
Yelets State University named after I. A. Bunin
(Yelets, Russian Federation)
lena.ocheretko@yandex.ru

PROBLEMS OF LEGAL REGULATION OF PUBLIC USE OF THE INTERNET, SOCIAL NETWORKS AND MEDIA RESOURCES

Abstract: In modern time, the Internet plays an important role for every person, penetrating into all areas of our activity. Convenience, comfort, speed – all these qualities of modern communication connections give any citizen ample opportunities for fruitful professional activity, stay in touch with relatives and friends for 24 hours, form an optimal search for the necessary information, help in catching offenders and solving crimes, further development of nano-technologies and other global processes; The Internet is ubiquitous. But, at the same time, the lack of legal regulation of any media resources and social networks, the missed mechanism of influence on offenders, the inability to prevent the dissemination of certain types of negative information as soon as possible – negate many of the advantages and opportunities of the Global Network. In this article, the author emphasizes the priorities in the legal regulation of relations in the field of public use of the Internet and suggests ways to improve these legal relations.

Keywords: media resources, public use of the Internet, social networks, messengers.

Анисимова Алина Сергеевна

Кандидат юридических наук, старший преподаватель кафедры информационного права и цифровых технологий,
Саратовская государственная юридическая академия
(г. Саратов, Российская Федерация)
saninp@rambler.ru

**К ВОПРОСУ О ПРАВОВОМ РЕГУЛИРОВАНИИ СЕТИ ИНТЕРНЕТ:
РЕАЛИИ 21 ВЕКА**

Аннотация: В статье рассматриваются вопросы, связанные с правовым регулированием Интернета в Российской Федерации. Отмечается его значимость для современного общества и государства в целом. В рамках статьи выделяются положительные и негативные тенденции в использовании Интернета. Последние годы все больше характеризуются оцифровкой различных сфер, путем внедрения различных технологий в человеческую деятельность. Спецификой большинства их них выступает то, что их действие напрямую взаимосвязано с Интернетом. В частности, в статье рассматривается вопрос использования технологий Интернета вещей, управление которыми осуществляется в том числе посредством сети.

Ключевые слова: Интернет, Интернет вещей, право, правовое регулирование, сертификация, цифровые технологии.

Для цитирования:

Анисимова А. С. К вопросу о правовом регулировании сети Интернет: реалии 21 века // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 224–229.

Развитие цифровых технологий XXI века определяет становление новой эпохи человечества, где особое место занимает Интернет, который уже сейчас делает удобной жизнь миллионов людей, образуя новый вид общественных отношений – интернет-отношений. Эти миллионы людей не представляют себя иначе, чем в качестве участников Интернета и правомерно считают себя частью уникального социально-виртуального пространства.

Вместе с тем, широкие возможности, предоставляемые

участникам интернет-отношений, способствуют появлению как положительных, так и отрицательных сторон в таком пространстве, что ведет к активизации процессов неконтролируемых отношений и негативно сказывается не только на состоянии Интернет-отношений, но и грозит безопасности.

Развитие положительного потенциала Интернета и его эффективное использование ведет к расширению возможностей, предоставляемых гражданам, среди них: обращение посредством сайтов в

Интернете в органы государственной власти, службу здравоохранения, получение услуг в электронном виде (оплата штрафов, коммунальных услуг и госпошлин, подача заявлений на регистрацию автотранспорта, подача заявления на оформление и выдачу загранпаспорта, заявление на регистрацию брака и др.), заключение различных договоров, оплата услуг через онлайн-банк и т. д. Интернет в значительной степени упрощает жизнь современного человека, что ведет как к экономии времени, так и сил. Происходит постепенный переход от «бумажных» дел к максимальной автоматизации.

В качестве отрицательных сторон Интернета выступают различные виды правонарушений, которые встречаются в виртуальном пространстве, среди них: мошенничество, клевета, доведение до самоубийства, организация террористических актов, взлом компьютерных систем, хакерские атаки и др. Вместе с тем, возрастающий профессионализм преступников и постоянное совершенствование технологий, и, как следствие, постоянная эволюция возможностей для совершения преступлений, создают новые вызовы для человечества.

Прогресс не стоит на месте – рынок информационных технологий постоянно пополняется новыми решениями – блокчейн, облачные технологии, большие данные, искусственный интеллект и другие. Сегодня как раз то время, когда

необходимо ответить на вопрос, какие из инновационных технологий могут быть применимы для повышения эффективности жизнедеятельности как отдельного человека, так и государства в целом, а также заложить в законодательство основы их использования в дальнейшем.

В 2020 году было принято Постановление Правительства РФ от 2 июля 2020 г. № 974 «О внесении изменений в некоторые акты Правительства Российской Федерации», которое закрепило перечень цифровых технологий, среди них:

- искусственный интеллект;
- новые производственные технологии;
- робототехника и сенсорика;
- интернет вещей;
- мобильные сети связи пятого поколения (цифровые сервисы);
- новые коммуникационные интернет-технологии;
- технологии виртуальной и дополненной реальности;
- технологии распределенных реестров;
- квантовые коммуникации;
- квантовые сенсоры;
- квантовые вычисления¹.

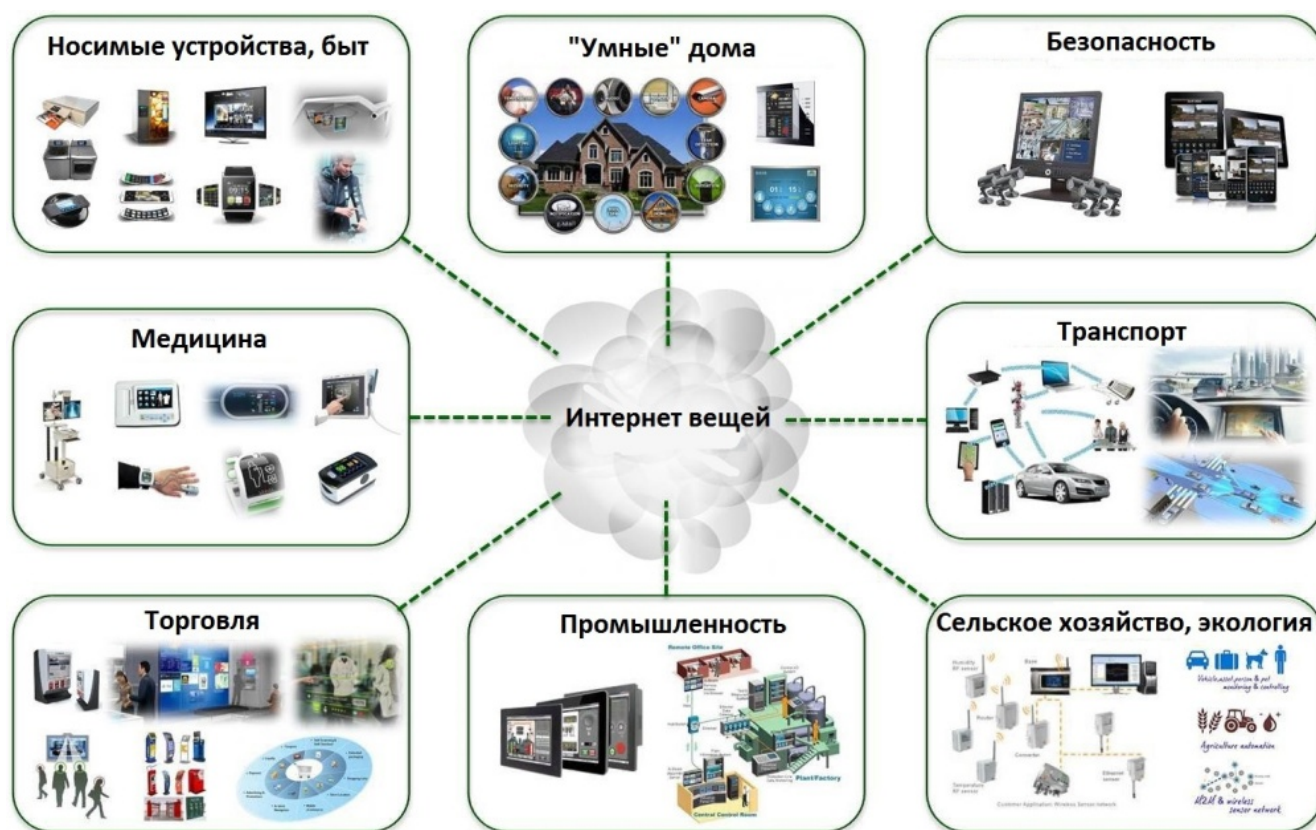
Большая часть из перечисленных технологий ориентированы в своей работе на использование Интернета. Так, особую актуальность на сегодняшний день представляет Интернет вещей. Он представляет собой системы, в которых Интернет подключается к

¹ См.: О внесении изменений в некоторые акты Правительства Российской Федерации: постановление Правительства РФ от 2 июля

2020 г. № 974 // Собрание законодательства Российской Федерации. 2020. Ст. 4426.

различным объектам, сенсорам и устройствам – вещам – чтобы они могли собирать и передавать информацию о своем окружении посредством программного обеспечения или же других устройств. Таким образом, устройства могут объединяться в сеть через Интернет или с помощью беспроводных технологий. Они обмениваются данными в режиме реального времени как напрямую, так и через удаленные онлайн-серверы (Рис. 1).

Рис. 1.



Таким образом, с помощью Интернета и телефона появляется возможность управлять различными технологиями. Сегодня использование Интернета вещей все больше наполняется правовым содержанием.

Однако, на сегодняшний день сеть Интернет не является «чистым», безопасным пространством, напротив, по мере развития самих цифровых технологий, растет количество преступлений, совершаемых с использованием таких технологий². Так, по данным Министерства внутренних дел число преступлений, которые были совершены в России в 2020 г. с использованием интернета, за год выросло на 91,3 %³. В связи с этим,

² См.: Жилкина С. А. Актуальные вопросы преступлений, связанных с использованием iot (интернета вещей) // Вопросы российской юстиции. 2020. № 6. С. 371–380.

³ См.: Число преступлений с использованием интернета выросло более чем на 91 % //

Ведомости. URL: <https://www.vedomosti.ru/society/news/2021/01/20/854794-chislo-prestuplenii-s-ispolzovaniem-interneta-viroslo-bolee-chem-na-91> (дата обращения: 10.05.2021).

не раз эксперты отмечали о главных опасностях Интернета вещей, так, в связи с использованием технологии «умного дома» ими выделяются следующие опасности:

1. DDoS-атаки (одновременное отправление огромного числа запросов с разных адресов с целью вывести из строя сервер или механизм).

2. Заражение экосистемы троянским ПО, последствия работы которого могут проявляться в краже личных фотографий, платежных данных или сканов документов.

3. Теоретически производитель (точнее его недобросовестный сотрудник) может оставить себе бэкдор и следить за вашим «умным домом» без вашего ведома. Такие случаи единичны, но они случались. Например, в январе признали виновным технического сотрудника американской компании ADT, который подсматривал за людьми через умные камеры наблюдения.

4. Совершенно точно периодически собирают информацию о том, что слышат, голосовые помощники (умные колонки). В дальнейшем эту информацию обрабатывают автоматически, чтобы повысить распознавание фраз искусственным интеллектом.

5. Майнинг в прошлом году пошел на спад, однако теперь, с ростом курса основных криптовалют, он снова может войти в моду. Принцип здесь такой же, как и с

ботнетом, только вирус другой: он сидит в фоне и заставляет смарт-ТВ, телефон или ноутбук добывать криптоденьги для неизвестного злоумышленника на другом конце света⁴.

Если в России рассматриваемые технологии еще не столь активно используются, то в ряде зарубежных стран уже можно встретить случаи их противоправного использования. Так, ноябре NBC News рассказал о случае, когда полиция отправилась в дом во Флориде после получения звонка от мужчины, заявившего, что он убил свою жену и хранил взрывчатку. Полицейские ничего не обнаружили и заявили, что кто-то «разыграл» их, используя «умный» дверной звонок; другой хакер взломал системы дома в Вирджинии и от имени владельца отправил сообщение полиции, что хочет совершить самоубийство. Приезд полиции злоумышленник транслировал на онлайн-платформах и брал \$ 5 за просмотр⁵.

Объединение домашних устройств в систему «умный дом» связано с повышенным риском взлома, так как, если хакеры проникнут в одно из устройств, они по цепочке смогут получить доступ ко всем остальным. Здесь возникает вопрос обеспечения безопасности, ведь, к примеру, количество взломов страничек в социальных сетях огромно, не приведет ли использование технологий интернета вещей к тому, что их взлом поставит

⁴ См.: Названы пять опасностей «умного» дома // Российская газета. 2021. 18 фев.

⁵ См.: Хакеры взламывают «умные» дома, вызывают спецназ и транслируют штурм в прямом эфире // Популярная механика. URL:

<https://www.popmech.ru/technologies/news-659363-hakery-vzlamyvayut-umnye-doma-vyzyvayut-specnaz-i-transliruyut-shturm-v-priyatom-efire/> (дата обращения: 10.05.2021).

под угрозу жизнь и здоровье человека, который этим пользуется.

В этой связи считаем, что, прежде чем внедрять технологии в жизнь, необходимо принимать комплекс мер по обеспечению безопасности их использования. В частности, это должны быть единые программные требования, которые будут обязательны для всех организаций, предлагающих подобные технологии. В Российской Федерации предпринимаются попытки на законодательном уровне разрешить данный вопрос. Так, в 2021 году были утверждены национальные стандарты в области технологий

интернета вещей, сенсорных сетей и промышленного интернета вещей, а также шесть нормативно-технических документов, регулирующих вопросы терминологии и типовых архитектур в Интернете вещей.

Безусловно, появление этих документов – важный шаг для развития в России новых продуктов с использованием технологии интернета вещей, однако достаточно ли будет таких норм для исключения возможности противоправного завладения цифровыми технологиями посредством Интернета покажет только время.

Список литературы

1. Жилкина С.А. Актуальные вопросы преступлений, связанных с использованием iot (интернета вещей) // Вопросы российской юстиции. 2020. № 6. С. 371-380.
2. Названы пять опасностей «умного» дома // Российская газета. 2021. 18 фев.
3. Хакеры взламывают «умные» дома, вызывают спецназ и транслируют штурм в прямом эфире // Популярная механика. URL: <https://www.popmech.ru/technologies/news-659363-hakery-vzlamyvayut-umnye-doma-vyzyvayut-sпецnaz-i-transliruyut-shturm-v-pryamom-efire/>.
4. Число преступлений с использованием интернета выросло более чем на 91 % // Ведомости. URL: <https://www.vedomosti.ru/society/news/2021/01/20/854794-chislo-prestuplenii-s-ispolzovaniem-interneta-viroslo-bolee-chem-na-91>.

Alina S. Anisimova

PhD (Law), Senior Lecturer

of the Department of Information Law and Digital Technologies,

Saratov State Law Academy

(Saratov, Russian Federation)

saninp@rambler.ru

ON THE ISSUE OF LEGAL REGULATION OF THE INTERNET: THE REALITIES OF THE 21ST CENTURY

Abstract: The article deals with issues related to the legal regulation of the Internet in the Russian Federation. Its significance for modern society and the state as a whole is noted. The article highlights the positive and negative trends in the use of the Internet. Recent years are increasingly characterized by the digitization of various spheres, through the introduction of various technologies in human activity. The specifics of most of them are that their action is directly interconnected with the Internet. In particular, the article deals with the use of technologies of Internet of Things that are managed through the network.

Keywords: Internet, Internet of Things, law, legal regulation, certification, digital technologies.

Анисимова Алина Сергеевна

Кандидат юридических наук, старший преподаватель кафедры информационного права и цифровых технологий,
Саратовская государственная юридическая академия
(г. Саратов, Российская Федерация)
saninp@rambler.ru

ТЕХНИКО-ПРАВОВЫЕ НОРМЫ РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ В СЕТИ ИНТЕРНЕТ

Аннотация: Статья посвящена вопросам правового регулирования отношений в Интернете. Обосновывается, что воздействие на интернет-отношения не может осуществляться исключительно нормами правовыми в том виде, как мы привыкли их видеть. Внимание необходимо уделять технической составляющей информационно-телекоммуникационной сети. Несмотря на то, что Интернет наполняют реальные люди, он имеет и другую сторону – технические компоненты, которые обеспечивают его работу. В этой связи актуальность выражается исследовании технико-правовых норм, упорядочивающих отношения в Интернете.

Ключевые слова: право, правовое регулирование, нормы права, технико-правовые нормы, Интернет, интернет-отношения.

Для цитирования:

Анисимова А. С. Техничко-правовые нормы регулирования отношений в сети Интернет // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 230–235.

Специфика сети, предоставляющей доступ в Интернет, заключается в том, что это многоуровневая система, где первостепенным началом выступают каналы связи, спутниковые каналы, системы доступа к сети. Следующий уровень – это уровень адресного пространства, доменных имен, доменных названий. Верхний уровень – это разного рода сервисы, поисковые системы, веб-сайты, социальные сети, почтовые системы, новостные сайты и т. д.

Таким образом, чтобы попасть на уровень пользователя Интернетом,

необходима эффективная и бесперебойная работа первых уровней, основной задачей которых выступает создание условий для непосредственного «вхождения» в виртуальное пространство.

В частности, за техническую составляющую Интернета отвечают:

1. Инженерный совет Интернета (IETF) – открытое международное сообщество проектировщиков, учёных, сетевых операторов и провайдеров, созданное в 1986 году и занимающееся развитием протоколов и архитектуры Интернета. Вся техническая работа

осуществляется в рабочих группах, занимающихся конкретной тематикой (например, вопросами маршрутизации, транспорта данных, безопасности и т. д.).

2. Сообщество Интернета (ISOC) – международная профессиональная организация (действует в 180 странах мира), занимающаяся развитием и обеспечением доступности сети Интернет¹. Принимает участие в решении широкого спектра вопросов, связанных с Интернетом, включая политику, управление, технологии и развитие. Основной целью организации выступает необходимость обеспечения надежного работоспособного доступа к Интернету для каждого нынешнего пользователя, а также для следующего миллиарда пользователей.

3. ICANN – некоммерческая организация, отвечающая за глобальную координацию системы уникальных элементов сети Интернет, т. е. распределение доменных имен, доменных названий (сейчас насчитывается порядка 250 национальных доменных имен). Таким образом, ICANN существует ради того, чтобы развивать и обеспечивать стабильность, безопасность и отказоустойчивость всемирного Интернета, а также занимается созданием новых программ доменных имен первого уровня.

4. Координационный центр национального домена сети Интернет

– администратор национальных доменов верхнего уровня RU и РФ. Основная деятельность заключается в обеспечении надежного и стабильного функционирования национальных доменов верхнего уровня RU и РФ. Выполняя функции национальной регистратуры, координационный центр реализует различные проекты, направленные на развитие и расширение использования Интернета в России в интересах российского и мирового интернет-сообществ².

Организации, работа которых заключается в создании, разработке и внедрении технических норм играют наиболее важную роль в работе Интернета. Осуществляя производственную деятельность, люди совершенствуют правила технологического, технического характера. Технические нормы представляют собой в первую очередь правила наиболее эффективного и рационального воздействия человека на окружающий мир, на природу в процессе производственной деятельности: правила сооружения здания, управления машинами и т. д. К ним также относятся нормы, определяющие способы оформления документации, организации учета и т. п. Указанные нормы имеют важное значение в деятельности государственных органов и общественных организаций.

Технические нормы – важнейший компонент в регулировании интернет-отношений, сущность которых заключается в

¹ См.: Internet Society. URL: <http://www.internetsociety.org/ru> (accessed: 01.01.2021).

² См.: Координационный центр национального домена сети Интернет. URL: <http://cctld.ru/ru/> (дата обращения 04.01.2021).

правильном использовании технических средств.

Еще в 1997 году во время Сессии по безопасности и сотрудничеству в Европе, фондом DIPLO'S CREATIVE LAB были разработаны основные аспекты управления Интернетом, одним из которых стали инфраструктура и стандартизация.

Инфраструктура и стандартизация включает в себя основополагающие технические вопросы, связанные с работой Интернета. Первая группа состоит из наиболее важных элементов, без которых Интернет не мог бы существовать: каналы связи, спутниковые каналы, системы доступа к сети и т. д. Как отмечает Д. Квотерман, с технической стороны Интернет представляет собой метасеть, состоящую из многих сетей, которые работают согласно протоколам семейства TCP/IP, объединены через шлюзы и используют единое адресное пространство и пространство имен³. TCP/IP – основной технический стандарт, определяющий способ передачи данных по Интернету. Семейство протоколов TCP/IP широко применяется во всем мире для объединения компьютеров. Единая сеть Интернет состоит из множества сетей различной физической природы, от локальных сетей типа Ethernet и Token Ring, до глобальных сетей типа NSFNET. Первый TCP/IP был установлен в Москве в 1993 году.

Особенность технических норм как элемента механизма правового

регулирования интернет-отношений главным образом заключается в том, что технические нормы могут в значительной степени дополнять действие правовых, что в конечном счете ведет к более эффективному воздействию.

Одним из примеров выступают системы фильтрации, которые заключаются в блокировке различной информации (порнографии, сцен насилия, пропаганды наркотиков и алкоголя, сайтов с азартными играми, мошенничества, вредоносного программного обеспечения, экстремизма, а также других ресурсов, доступ к которым должен быть ограничен в соответствии с законодательством Российской Федерации и т. д.).

Вместе с тем, применение в учебных заведениях контент-фильтров является обязанностью руководства таких учреждений. Еще с 1 апреля 2008 г. в рамках национального приоритетного проекта «Образование» российские школы были обеспечены лицензионными компьютерными программами и системой фильтрации доступа в Интернет, цель которых заключалась в ограничении доступа обучающихся образовательных учреждений к ресурсам Интернета, содержащим информацию, не совместимую с задачами образования.

В целях совершенствования технических норм, регулирующих Интернет, в 2011 г. были разработаны «Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации

³ См.: Quarterman J. The Matrix: Computer Networks and Conferencing Systems

Worldwide. Bedford, MA: Digital Press, 1990. P. 401.

доступа к Интернету, реализованной Министерством образования и науки Российской Федерации», которые закрепили основные требования, которым должны соответствовать такие системы, а также под средствами контент-фильтрации доступа к сети Интернет представили аппаратно-программные или программные комплексы, обеспечивающие ограничение доступа к интернет-ресурсам, не совместимым с задачами образования и воспитания обучающихся⁴.

В 2014 г. были разработаны Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, которые закрепили: виды информации, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования; требования к техническим и программно-аппаратным средствам защиты детей от видов информации; систему организационно-административных мероприятий, направленных на защиту детей от видов информации и ряд других вопросов⁵.

⁴ См.: Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации (утв. Минобрнауки России 11.05.2011 № АФ-12/07вн) // СПС «КонсультантПлюс».

⁵ См.: О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет (вместе с «Методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой

Таким образом, технические нормы в механизме правового регулирования интернет-отношений играют важную роль, к ним можно отнести любые вспомогательные нормы, регулирующие права и обязанности сторон правоотношения. Специфика таких технических норм заключается, прежде всего, в их масштабности, несмотря на то, что программа устанавливается на один компьютер, она блокирует информацию со всей страны; быстрота внедрения: достаточно нескольких часов для ее оптимизации на компьютере; защита от вредоносного программного обеспечения.

Однако, реализация проектов, различных инициатив и программ, увеличивающих наши возможности в Интернете и обеспечивающих безопасность, невозможна без поддержания юридическими нормами. Существует объективная потребность в заключении договоров и принятии норм, регламентирующих влияние телекоммуникаций на интернет-отношения.

Например, после разработки стандарта беспроводной связи Wi-Fi и

посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования», «Рекомендациями по организации системы ограничения в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования»): письмо Минобрнауки России от 28.04.2014 № ДЛ-115/03 // Администратор образования. 2014. № 24.

распространения его действия на территории всего государства было принято

Постановление Правительства Российской Федерации от 31 июля 2014 г. № 758 «О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей», согласно которому доступ к общественным точкам с доступом в Интернет (где можно воспользоваться интернетом с чужого компьютера: компьютерных клубов, интернет-кафе, отделения почты России и т. д.), может осуществляться только после идентификации пользователей. Для этого оператор должен получить от пользователя его ФИО, подтверждённые документом, удостоверяющим личность⁶.

Согласно изменениям, общественное заведение, предоставляющее доступ в Интернет со своих устройств, обязано формировать реестр посетителей, который в случае необходимости необходимо будет предоставить правоохранным органам. Тем самым, если пользователь распространяет в интернет-кафе запрещенный контент (призывы к насилию, распространение наркотиков и т. д.), процесс его опознания упрощается, поскольку уже имеется информация о таком посетителе. Такие действия были приняты в рамках пакета законопроектов, ужесточающих меры против терроризма.

Следовательно, спецификой правового регулирования отношений в Интернете выступает то, что необходимо использовать как правовые нормы, так и нормы технические, которые в совокупности будут обеспечивать взаимосвязь, позволяющей поддерживать наше право на общение и получение информации в нужном виде, а также обеспечение безопасности.

Список литературы

1. Quarterman J. The Matrix: Computer Networks and Conferencing Systems Worldwide. Bedford, MA: Digital Press, 1990.

⁶ См.: О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам

упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей: постановление Правительства Российской Федерации от 31 июля 2014 г. № 758 г. // Собрание законодательства Российской Федерации. 2014. № 32. Ст. 4525.

Alina S. Anisimova

PhD (Law), Senior Lecturer

of the Department of Information Law and Digital Technologies,

Saratov State Law Academy

(Saratov, Russian Federation)

saninp@rambler.ru

TECHNICAL AND LEGAL REGULATION OF RELATIONS IN THE INTERNET

Abstract: The article is devoted to the issues of legal regulation of relations on the Internet. It is substantiated that the impact on Internet relations cannot be carried out exclusively by legal norms in the form we are used to seeing them. Attention must be paid to the technical component of the information and telecommunications network. Despite the fact that the Internet is filled with real people, it also has another side – the technical components that make it work. In this regard, the relevance is expressed by the study of technical and legal norms that regulate relations on the Internet.

Keywords: law, legal regulation, legal norms, technical and legal norms, Internet, Internet relations.

Жилиева Александра Михайловна

Магистрант,

Орловский государственный университет им. И. С. Тургенева

(г. Орёл, Российская Федерация)

alexandrzhilyaeva2016@mail.ru

Научный руководитель – Л. А. Абашина, кандидат юридических наук,
зав. кафедрой уголовного права

НЕКОТОРЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ В СЕТИ ИНТЕРНЕТ

Аннотация: На сегодняшний день Всемирная паутина является площадкой распространения идеологии терроризма. В статье рассматривается состав преступления, предусмотренного статьей 205.2 Уголовного кодекса Российской Федерации как характерное преступление террористической направленности, совершаемое при помощи сети Интернет. Кроме того, уделяется внимание обнаружению противоправного контента и его последующей блокировки.

Ключевые слова: сеть Интернет, противодействие, терроризм, вербовка, материалы.

Для цитирования:

Жилиева А. М. Некоторые аспекты противодействия терроризму в сети Интернет // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 236–240.

Как отмечается в Стратегии противодействия экстремизму в Российской Федерации до 2025 года, информационно-коммуникационные сети, включая сеть «Интернет», стали основным средством коммуникации для экстремистских и террористических организаций, которые используются для привлечения в свои ряды новых членов данных организаций, а также для организации и координации

совершения преступлений экстремистской и террористической направленности, распространения экстремистской идеологии¹. Задача информационного противодействия терроризму и экстремизму приобретает особую значимость в системе мер борьбы с данными угрозами.

Говоря о распространении информации террористическими организациями, стоит отметить такое

¹ Стратегия противодействия экстремизму в Российской Федерации до 2025 года от 28.11.2014 № Пр-2753 // СПС

«КонсультантПлюс». URL: www.consultant.ru/document/cons_doc_LAW_194160 (дата обращения: 15.05.2021).

уголовно наказуемое деяние, как публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма – статья 205.2 Уголовного кодекса Российской Федерации (далее – УК РФ), и проанализировать состав данного преступления.

Так, объект преступления – общественная безопасность. Объективная сторона данного деяния выражается в совершении следующих альтернативных действий: а) публичные призывы к осуществлению террористической деятельности; б) публичное оправдание терроризма; в) пропаганда терроризма.

Стоит заметить, что призывы должны носить конкретный характер и побуждать именно к террористической деятельности. Призывы и заявления могут быть как устными, так и посредством изготовления и распространения печатных материалов, в том числе и через сеть Интернет². Призывы по своему содержанию схожи с подстрекательством.

Субъективная сторона преступления выражена также прямым умыслом. Согласно части 1 статьи 20 УК РФ, субъект преступления – физическое вменяемое лицо, достигшее возраста 16 лет³.

Квалифицирующим признаком состава преступления является его совершение с использованием средств

массовой информации, в том числе сети Интернет (часть 2 статьи 205.1 УК РФ). При совершении такого преступления, помимо УК РФ, необходимо руководствоваться Законом Российской Федерации № 2124-1 «О средствах массовой информации». Так, согласно статье 4 данного закона, закреплен запрет на распространение материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм⁴.

Кроме того, как справедливо замечает С. М. Кочои, при совершении публичных призывов к осуществлению террористической деятельности путем массовой рассылки сообщений абонентам мобильной связи или с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», преступление следует считать оконченным с момента размещения обращений в сетях общего пользования (на сайтах, блогах), отправления сообщений другим лицам⁵.

Собственно основными видами информационных ресурсов, которые используются в террористической и экстремистской деятельности, являются: 1) средства массовой информации; 2) интернет-ресурсы; 3) средства мобильной связи; 4) навигационные аппаратно-

² Рарог А. И. Уголовное право России: учебник. М.: Проспект, 2019. С. 610.

³ Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 05.04.2021) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

⁴ О средствах массовой информации: закон РФ от 27.12.1991 № 2124-1 (ред. от 01.01.2021) // Российская газета. 1992. 8 фев. № 32.

⁵ Антиэкстремистские нормы: моногр. / под ред. М. С. Кочои. М.: Проспект, 2020. С. 137.

программные приборы. Однако данный перечень не является исчерпывающим; он дополняется по мере развития информационно-телекоммуникационные технологий.

Обширная аудитория и колоссальные возможности распространения информации привели к тому, что все террористические организации являются пользователями сети Интернет. Так, по мнению В. В. Меркурьева, к наиболее активным террористическим организациям, целенаправленно использующим ресурсы Интернета, можно отнести: «Братья мусульмане», «Исламское государство», «Народный фронт освобождения Палестины», «Аль-Джихад» и многие другие⁶.

Также в российском сегменте Интернета экстремистские и террористические интернет-сайты пропагандируют политические идеи, проводят агитационную и вербовочную деятельность, которая и направлена на увеличение числа своих сторонников.

Как отмечает официальный представитель Национального антитеррористического комитета Андрей Пржездомский, происходит трансформация террористической деятельности. Это – вербовка через Интернет, спящие ячейки, теракты, осуществляемые подручными средствами. Еще в 2017 году он подчёркивал, что некоторые

противоправные действия террористических организаций осуществляются дистанционно, то есть удаленно. Процесс бывает очень быстрым, воздействие иногда происходит за несколько месяцев. И в настоящее время ни один теракт не обходится без использования социальных сетей, причем вербовкой у террористов занимаются «специалисты самого высокого профиля».

Кроме того, правоохранительные органы производят мониторинг социальных сетей. Здесь огромную роль играет взаимодействие Роскомнадзора и правоохранительных органов в пресечении распространения террористической пропаганды в сети Интернет. В данных целях и функционирует Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено⁷. Это одно из полномочий Федеральной служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, согласно п. 5.1.7 Постановления Правительства РФ № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и

⁶ Борьба с терроризмом: новые вызовы и угрозы: моногр. / под ред. В. В. Меркурьева. М.: Проспект, 2020. С. 236.

⁷ Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать

сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено. URL: <https://eais.rkn.gov.ru/> (дата доступа: 12.05.2021).

массовых коммуникаций». Так, за последние годы в Российской Федерации был заблокирован и удалён противоправный контент с более чем 60000 сайтов, более 10000 страниц оказались внесёнными в число запрещённых. На некоторых ресурсах зачастую размещаются и агитационные материалы с призывами оказывать финансовую помощь террористическим группам с указанием номеров мобильных телефонов, QIWI-кошелек и иных платежных реквизитов.

Помимо этого, существует Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет, который ведет активную работу в сфере выявления противоправного контента. Данный центр анализирует информацию в поисковых системах, а затем передает материалы для дальнейшего анализа и блокировки правоохранительным органам. Например, в период с января по декабрь 2020 года сотрудниками центра было выявлено 709 ссылок на противоправный контент, 424 из них – ссылки на экстремистские и террористические материалы⁸.

В статье Н. В. Володиной приводится мнение таких учёных, как

Н. Ю. Григорьев и Э. Ю. Родюков. Они вводят понятие информационного терроризма⁹. Так, под этим понятием они подразумевают форму негативного воздействия на личность, общество и государство всеми видами информации. Он ведется разнообразными силами и средствами – от агентуры иностранных спецслужб до отечественных и зарубежных средств массовой информации. Терроризм – форма психологической войны посредством сети Интернет. Ведь именно сеть Интернет стала основным каналом распространения экстремистских и террористических идей, побуждающих совершать преступные деяния.

Таким образом, наращивание темпов внедрения информационно-телекоммуникационных технологий во все сферы жизни общества и государства способствует появлению новых угроз государственной и общественной безопасности. Прогнозируется, что информационно-телекоммуникационные технологии будут использоваться не только для совершения преступлений террористической направленности, но и станут фактором трансформации традиционных видов преступлений.

⁸ Официальный сайт Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет: отчеты деятельности. URL: <https://ncpti.su/report/monitoring->

[seti/monitoring-seti-internet.php](https://ncpti.su/report/monitoring-seti/monitoring-seti-internet.php) (дата доступа: 12.05.2021).

⁹ Володина Н. В. Деятельность «Исламского государства» («ИГ») как угроза конституционной безопасности // Российский следователь. 2015. № 3. С. 43.

Список литературы

1. Антиэкстремистские нормы: моногр. / под ред. М. С. Кочои. М.: Проспект, 2020. 200 с.
2. Борьба с терроризмом: новые вызовы и угрозы: моногр. / под ред. В. В. Меркурьева. М.: Проспект, 2020. 680 с.
3. Володина Н. В. Деятельность «Исламского государства» («ИГ») как угроза конституционной безопасности // Российский следователь. 2015. № 3. С. 43–47.
4. Рарог А. И. Уголовное право России: учебник. М.: Проспект, 2019. 895 с.

Aleksandra M. Zhilyaeva

Graduate student,

Orel State University named after I. S. Turgenev

(Orel, Russian Federation)

alexandrazhilyaeva2016@mail.ru

Scientific supervisor – L. A. Abashina, PhD (Law), Head of the Department of Criminal Law

SOME ASPECTS OF COUNTERING TERRORISM ON THE INTERNET

Abstract: Today, the World Wide Web is a platform for spreading the ideology of terrorism. The article considers the composition of the crime provided for in Article 205.2 of the Criminal Code of the Russian Federation as a characteristic crime of a terrorist nature committed using the Internet. In addition, attention is paid to the detection of illegal content and its subsequent blocking.

Keywords: the Internet, counteraction, terrorism, recruitment, materials.

УДК 343.72

Богатырева Софья Викторовна

Студент,

Южно-Уральский государственный университет

(г. Челябинск, Российская Федерация)

sofia.bogatyreva.7778@mail.ru

Научный руководитель – Т. И. Ястребова, кандидат юридических наук, доцент
кафедры уголовного процесса, криминалистики и судебной экспертизы

ПРОБЛЕМЫ РАСКРЫТИЯ МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ С ИСПОЛЬЗОВАНИЕМ ФИШИНГОВЫХ САЙТОВ И ПУТИ ИХ РЕШЕНИЯ

Аннотация: В данной статье проанализирован такое относительно новое средство совершения мошенничества в сети Интернет как фишинг. Данное средство совершения преступления на настоящий момент законодательно не урегулировано, в связи с чем выявление и пресечение на практике представляет определенные трудности. Внесены предложения по выявлению и возможному предотвращению мошеннических действий с использованием фишинговых сайтов.

Ключевые слова: преступление, мошенничество, блокирование, разделение, фишинговые сайты, информационные технологии.

Для цитирования:

Богатырева С. В. Проблемы раскрытия мошенничества в сети Интернет с использованием фишинговых сайтов и пути их решения // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 241–245.

Развитие и совершенствование информационных технологий помимо неопределимых достоинств внесли и ряд достаточно больших проблем. Это касается преступности, которая никогда не стоит на месте, а продолжает видоизменяться и приспособливаться к новым реалиям.

С появлением глобальной сети Интернет преступники перешли в цифровое поле, придумывая все более

и более изощренные способы мошеннических действий. По статистическим данным МВД России за период с января по декабрь 2020 года преступлений с использованием сети Интернет возросло на 91,3 %¹. И это только данные зарегистрированных преступлений, уровень же латентных преступлений неизвестен. Этот огромный отрицательный показатель доказывает

¹ Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2020 года // Министерство внутренних дел РФ: официальный сайт.

URL: <https://xn--blaew.xn--plai/reports/item/22678184/> (дата обращения: 12.04.2021).

неэффективность проведения мер по выявлению и пресечению таких преступлений.

Низкая раскрываемость данного вида преступлений связана с тем, что порой не хватает доказательств для подтверждения вины преступника либо ресурсов для вычисления его местоположения².

Мошеннические действия в сети Интернет очень разнообразны, это могут быть как «двойники» социальных сетей, где от пользователя требуют ввести пароль, сообщения от неизвестных людей, содержащие подозрительные ссылки для якобы получения какого-либо выигрыша или денежный выплат³.

Однако, часто для совершения преступлений создаются так называемые «фишинговые» сайты. Как правило, такие сайты либо практически полностью дублируют официальные сайты, например, «Сбербанк», меняя в официальном названии несколько символов, либо создают поддельные сайты, специализирующиеся якобы на продаже каких-либо товаров или услуг. Часто фишинговые сайты можно встретить при покупке авиабилетов и билетов на поезда, на концерты, в театры и т. д.

В период с января по сентябрь 2017 года служба кибербезопасности Сбербанка выявила и заблокировала 600 фишинговых сайтов⁴. Также выявлением фишинговых сайтов занимаются Национальный координационный центр по компьютерным инцидентам, Group-IB, Лаборатория Касперского, RU-CERT, Банк России и Доктор Веб⁵.

Бороться с фишинговыми сайтами можно двумя способами: путем блокировки либо разделегированием домена. Последний способ наиболее эффективен, поскольку, если после блокировки сайта еще существуют возможности обойти ее и таким образом сайт еще сможет существовать, то при разделегировании домена администратор полностью лишается способности управления сайтом.

Разделегирование доменов может происходить как в судебном, так и внесудебном порядке. В частности, в судебном порядке решаются вопросы о разделегировании доменов, если его администратор нарушил право интеллектуальной собственности.

Разделегирование доменов во внесудебном порядке происходит в

² Жуков С. Карты сдали: новые атаки мошенников на наши электронные кошельки // Российская газета. 2020. 9 фев. URL: <https://rg.ru/2020/02/05/internet-moshenniki-pridumali-novye-sposoby-obmana.html> (дата обращения: 15.04.2021).

³ Некрасова Т. Н. Анализ влияния недобросовестных практик на рынок финансовых услуг // Известия Санкт-Петербургского государственного экономического университета. 2020. № 1. С. 164.

⁴ Бахур В. Сбербанк выявил более 600 фишинговых доменов и 1300 распространявших вирусы сайтов // CNews. 2017. 5 сен. URL: https://safe.cnews.ru/news/line/2017-09-15_sberbank_vyyavil_bole_600_fishingovyh_domenov (дата обращения: 17.04.2021).

⁵ Официальный сайт Координационного центра доменов .RU/.РФ: URL: <https://cctld.ru/help/safety/> (дата обращения: 18.04.2021).

соответствии с «Правилами регистрации доменных имён в доменах .RU и .РФ»⁶. В частности, п. 5.5 данных правил содержит указание на то, что на основании письменного решения руководителя органа, осуществляющего оперативно-розыскную деятельность, регистратор делегирует домен.

Однако несмотря на то, что правоохранительные органы могут влиять на снижение уровня фишинговых сайтов, уровень преступлений не уменьшается. В связи с чем целесообразно предложить новое решение в данной сфере.

Как правило, основной упор делается на информационную и правовую грамотность рядовых пользователей – при появлении сомнений о достоверности сайта он сообщает в одну из компетентных организация (Group-IB и др.).

В ведении Роскомнадзора находится «Единый реестр доменных имён, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»⁷. Федеральный закон от 27.07.2006 № 149-ФЗ «Об

информации, информационных технологиях и о защите информации» в ч. 5 ст. 15.1 устанавливает основания, при наличии которых доменные имена и сетевые адреса вносятся в данный реестр⁸.

При помощи такого реестра любой пользователь может узнать содержится ли тот или иной сайт в реестре или нет.

Для борьбы с мошенничеством, осуществляемым с помощью фишинговых сайтов, на наш взгляд, также целесообразно создание особого реестра. Такой реестр должен находиться в ведении Министерства внутренних дел. Цель создания: включение в такой реестр сайтов, социальных сетей и т. д., где используются платёжные системы.

Другие правоохранительные органы имеют отдельные полномочия по борьбе с информационными преступлениями, например, Приказом ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» был создан НКЦКИ, в полномочия которого входит противодействие кибератакам на критическую информационную

⁶ Правила регистрации доменных имен в доменах .RU и .РФ: решение Координационного центра национального домена сети Интернет от 05.10.2011 № 2011-18/81 (с изм. и доп.) // Официальный сайт Координационного центра доменов .RU/.РФ. URL: https://cctld.ru/files/pdf/docs/rules_ru-rf.pdf (дата обращения: 16.04.2021).

⁷ Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие

информацию, распространение которой в Российской Федерации запрещено: постановление Правительства РФ от 26.10.2012 № 1101 (с изм. и доп.) // СПС «Гарант». URL: <https://base.garant.ru/70248270/> (дата обращения: 18.04.2021).

⁸ Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ (с изм. и доп.) // СПС «Гарант». URL: <https://base.garant.ru/12148555/> (дата обращения: 22.04.2021).

инфраструктуру⁹. В частности, в полномочия НКЦКИ входит блокирование и разделегирование доменов тех сайтов, которые могут представлять угрозу.

В связи с чем, наделение МВД России дополнительными полномочиями по борьбе с киберпреступностью, на наш взгляд, вполне уместно.

Мы полагаем, что целесообразно наделить полномочиями по ведению реестра сайтов с платежными системами Управление «К» МВД России, поскольку данное управление как раз в пределах своей компетенции осуществляет выявление, предупреждение, пресечение и раскрытие преступлений в сфере компьютерной информации, а в частности, как раз мошенничество в сфере компьютерной информации. Данные полномочия должны быть оформлены приказом МВД России и устанавливать сроки, в течение которых администраторы сайтов, на которых имеются платежные системы, подать заявку на включение их сайта в реестр. Сотрудники Управления «К» проводят проверку таких сайтов на предмет законности проведения платежных операций.

После истечения установленных сроков сотрудники Управления «К» будут заниматься мониторингом сети «Интернет» и разделегировать домены сайтов с незаконными платежными системами.

Первоначально, мониторинг должен быть на выявление сайтов-двойников и реагирование на жалобы пользователей, позже на поиск иных сайтов, не входящих в реестр, где применяются платежные системы.

Данное полномочия Управления «К» МВД России должно быть закреплено в «Правилах регистрации доменных имен в доменах .RU и .РФ», в частности, в пункте 5.7.

Таким образом, создание приказом МВД реестра сайтов с легальными платежными системами и наделение полномочиями Управление «К» Министерства внутренних дел по обеспечению функционирования такого реестра позволит ограничить круг сайтов с легальными платежными системами, что позволит рядовым пользователям при оплате товаров/работ/услуг обратиться к данному реестру и не попасться на уловки мошенников.

Список литературы

1. Бахур В. Сбербанк выявил более 600 фишинговых доменов и 1300 распространявших вирусы сайтов // CNews. 2017. 5 сен. URL: https://safe.cnews.ru/news/line/2017-09-15_sberbank_vyyavil_bolee_600_fishingovyh_domenov.

⁹ Курбатов Н. М. Изменения в нормативном правовом регулировании обеспечения безопасности критической информационной

инфраструктуры Российской Федерации // Вестник Удмуртского университета. Серия «Экономика и право». 2019. № 3. С. 405.

2. Жуков С. Карты сдали: новые атаки мошенников на наши электронные кошельки // Российская газета. 2020. 9 фев. URL: <https://rg.ru/2020/02/05/internet-moshenniki-pridumali-novye-sposoby-obmana.html>.

3. Курбатов Н. М. Изменения в нормативном правовом регулировании обеспечения безопасности критической информационной инфраструктуры Российской Федерации // Вестник Удмуртского университета. Серия «Экономика и право». 2019. № 3. С. 401–409.

4. Некрасова Т. Н. Анализ влияния недобросовестных практик на рынок финансовых услуг // Известия Санкт-Петербургского государственного экономического университета. 2020. № 1. С. 163–166.

Sofia V. Bogatyreva

Student,

South Ural State University
(Chelyabinsk, Russian Federation)
sofia.bogatyreva.7778@mail.ru

Scientific supervisor – T. I. Yastrebova, PhD (Law), Associate Professor of the
Department of Criminal Process, Forensics and Forensic Expertise

PROBLEMS OF DISCLOSURE OF FRAUD ON THE INTERNET WITH THE USE OF PHISHING SITES AND THE WAYS OF THEIR SOLUTION

Abstract: This article analyzes such a relatively new means of committing fraud on the Internet as phishing. This means of committing a crime is currently not amenable to legal regulation, in connection with which identification and suppression is problematic. In this connection, it is important to identify regulatory means of solving fraud using phishing.

Keywords: crime, fraud, blocking, de-delegation, phishing sites, information technology.

Судариков Дмитрий Николаевич

Магистрант,

Поволжский институт (филиал) Всероссийского государственного университета
юстиции (РПА Минюста России)

(г. Саратов, Российская Федерация)

sudarikovfssp64@yandex.ru

Научный руководитель – Богомолова К. И., кандидат юридических наук

ПРОБЛЕМЫ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ В БОРЬБЕ С ЭКСТРЕМИЗМОМ И ПУТИ ИХ РЕШЕНИЯ

Аннотация: В данной статье рассматриваются текущее состояние и проблемы международного сотрудничества правоохранительных органов в борьбе с экстремизмом как сдерживающего фактора противодействия преступлениям экстремистской направленности. Анализируется взаимодействие Российской Федерации с иностранными государствами, международными и региональными организациями в области противодействия экстремизму, а также разрабатываются основные пути решения имеющихся проблем.

Ключевые слова: экстремизм, международное сотрудничество, антитеррористическое сотрудничество, терроризм, борьба с терроризмом, правоохранительные органы, международное сотрудничество правоохранительных органов.

Для цитирования:

Судариков Д. Н. Проблемы международного сотрудничества правоохранительных органов в борьбе с экстремизмом и пути их решения // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 246–252.

Экстремизм, как явление, происходит там, где для этого существуют определенные условия. К данным условиям могут относиться:

- 1) полиэтнический состав стран;
- 2) многоконфессиональность;

- 3) социальное неравенство;
- 4) неустойчивость политических систем в государствах;
- 5) слабость и неготовность силовых структур;
- 6) природные условия¹.

¹ Сералиев А. Б. Правовое обеспечение противостояния терроризму и экстремизму: концептуальные подходы формирования

национального законодательства // Четвертые юридические чтения. Сборник статей. 2017. С. 172.

Список условий можно продолжить, так как именно устранение данных условий является первой задачей в борьбе с экстремизмом. Но международный экстремизм и отличается тем, что он характерен для всех стран, а если это так, то и борьба с ним носит общий характер.

В настоящее время все большее влияние на процессы, протекающие в современном мире, оказывает экстремизм. Именно он, являясь социально-политическим явлением, несет в себе угрозы безопасности, как отдельному государству, так и всему миру. Эти угрозы представляют собой конкретные и непосредственные проявления деструктивных факторов, порождаемые целенаправленной деятельностью террористических сил, имеют внутренний и внешний характер, являются нарастающими, постоянными, общенациональными, реальными, а по силе воздействия – сильными или критическими.

Современные тенденции в области распространения экстремизма и терроризма весьма негативны. Опасения вызывает не просто количественный рост преступлений данного вида. Данная угроза приобрела в последние несколько лет качественно новое, еще более тревожное измерение, связанное с появлением и развитием международных террористических группировок (так называемое Исламское Государство и Джебхат ан-

Нусра (запрещены в России)), поднявших террористическое насилие на невиданный уровень жестокости².

Негативной тенденцией также является широкое использование преступниками возможностей сети Интернет при совершении преступлений террористической и экстремистской направленности. Развитие информационно-коммуникационных технологий привело к массовому их использованию, в том числе для пропаганды экстремистских идей. И как следствие большое число преступлений совершается посредством сети Интернет. Так, по данным ГИАЦ МВД России, практически 30 % преступлений экстремистской направленности совершены с использованием сети Интернет.

Совершенствование Интернета открывает не только новые возможности, но и новые глобальные угрозы для мирового сообщества. Террористические организации активно используют средства сети Интернет для связи и обмена информацией, ведения пропаганды и вербовки новых членов. Рамзи Юзеф, организатор взрывов Всемирного торгового центра в Нью-Йорке 11 сентября 2001 г., получал по Интернету зашифрованные послания-инструктажи от Усамы бен Ладена.

В конце XX в. появилось совершенно новое явление в сфере информационных технологий –

² Мухтаров М. М., Ергенбек У. Е. Использование социальных сетей для выявления лиц, причастных к экстремистской деятельности // Эффективное государство: достижения и

новые направления развития: сборник научных трудов по материалам I Международной научно-практической конференции. 2017. С. 112.

компьютерный или кибертерроризм, т. е. использующий для достижения своих преступных целей компьютеры, электронные сети и современные информационные технологии.

Компьютерный терроризм проявляется в двух аспектах — технологическом и информационном. Технологический аспект компьютерного терроризма связан с технологической формой проявления различных видов терроризма — использованием компьютерных технологий для совершения террористических действий (выведение из строя или разрушение опасных объектов, получение контроля над потенциально опасными объектами, создание условий для аварий и катастроф техногенного характера и пр.).

Информационный аспект связан с осуществлением воздействия на психику и сознание общества с целью формирования нужных мыслей и суждений, определенным образом направляющих поведение людей в нужном для террористов направлении. При этом компьютеры, компьютерные системы и сети выполняют роль средства доставки такой информации до потребителей — пользователей глобальных сетей.

В современный период особое значение приобретают вопросы, связанные с противодействием экстремизму и терроризму, в рамках СНГ, ОДКБ и ШОС, а также в других формах международного сотрудничества. Важным

юридическим документом СНГ в антитеррористической сфере является Договор о сотрудничестве государств-участников СНГ в борьбе с терроризмом от 04.06.1999 г. (ратифицирован Россией 28.12.2004 г.), в котором участвуют Азербайджан, Армения, Беларусь, Казахстан, Киргизия, Молдова, Россия, Таджикистан. Договором (ст. 2) предусматривается, что стороны обязуются сотрудничать по вопросам борьбы с терроризмом в соответствии с договором, национальным законодательством и международными обязательствами³.

Российская Федерация твердо исходит из того, что с глобальной террористической угрозой надо бороться сообща, на подлинно коллективной основе, во взаимодействии. Применительно к теме международного сотрудничества правоохранительных органов, без которого невозможно представить эффективного противодействия терроризму и экстремизму, то в настоящее время можно выделить ряд тенденций.

Так, основными направлениями деятельности международного сообщества по профилактике международного терроризма является комплекс мер, а именно: политические, идеологические, социально-экономические, правовые, специальные, военные и т. д. К примеру, важным инструментом взаимодействия на пространстве СНГ является Совет министров внутренних

³ Шхагапсоев З. Л., Бураева Л. А. Об актуальных вопросах международного сотрудничества в противодействии проявлениям экстремизма и терроризма в

интернет-пространстве // Пробелы в российском законодательстве. 2018. № 5. С. 253.

дел государств – участников Содружества. Органами внутренних дел совместно реализуется ряд межгосударственных программ в сфере правоохранительной направленности. В том числе в сфере борьбы с экстремизмом, незаконным оборотом наркотиков, торговлей людьми, нелегальной миграцией.

Наиболее тесные связи у российских правоохранителей налажены с коллегами из стран Евразийского экономического союза. С ними образованы объединённые коллегии, где на ежегодных заседаниях рассматриваются актуальные вопросы противодействия общим вызовам и угрозам экстремистского характера.

Кроме того, в международной антитеррористической деятельности Российская Федерация тесно взаимодействует с Контртеррористическим комитетом, созданным на основе Резолюции Совета Безопасности ООН от 28 сентября 2001 года № 1373 и опирается на принятую Генеральной Ассамблеей ООН в сентябре 2006 года Глобальную Контртеррористическую стратегию. В данной Стратегии отражены такие задачи, как развитие идеи противодействия террористической идеологии и запрета подстрекательства к совершению преступлений террористической направленности, подключения гражданского общества к противодействию терроризму и

поощрения межкультурного диалога, культуры мира, религиозной и конфессиональной терпимости⁴.

Помимо этого, развито сотрудничество с зарубежными полицейскими структурами активно развивается в рамках Интерпола. С использованием возможностей этой организации за рубежом установлено местонахождение ста семидесяти семи обвиняемых, скрывшихся от российских правоохранительных органов. На территорию нашего государства экстрадировано и депортировано 64 разыскиваемых за совершение экстремистских преступлений лица.

Тем не менее, на сегодняшний день существуют определенные проблемы в области совместной деятельности по противодействию терроризму и экстремизму.

В первую очередь, к таковым следует отнести политически мотивированные ограничения на реализацию таких эффективных форм взаимодействия, как обмен информацией, силами и средствами, совместное проведение оперативно-розыскных операций, розыск и экстрадиция подозреваемых и обвиняемых в совершении преступлений экстремистской и террористической направленности и т. п.

Так, к большому сожалению, стоит отметить, что сотрудничество по вопросам борьбы с экстремизмом и терроризмом в формате Россия –

⁴ Карими Х. Х. Правовые вопросы взаимодействия в области уголовного преследования // Наука как движущая антикризисная сила: инновационные преобразования, приоритетные направления

и тенденции развития фундаментальных и прикладных научных исследований: сборник научных статей по итогам международной научно-практической конференции. 2016. С. 209.

НАТО, начатое после трагических событий в США 2001 года и ряда террористических актов на территории России и продолжавшееся до 2008 года, в настоящее время не имеет такой активности. Связано это, в первую очередь, приостановкой деятельности Совета Россия – НАТО из-за возникшего конфликта между Россией и Грузией⁵.

Постоянные попытки определенных сил на Западе сменить правящие режимы в арабских государствах, косвенное содействие созданию и организации Исламского государства (ИГИЛ), устроившей кровавую бойню в Сирии, Ираке, Ливане и близлежащих странах, организация и раздувание вооруженных конфликтов в регионах, граничащих с Российской Федерацией (Грузия, Украина) вызывают все больше политических противоречий и всё больше мешают объединению стран в целях борьбы с экстремизмом.

Правительства стран и ответственные лица, на сегодняшний день, все чаще стараются избежать контактов с «потенциальными противниками» и их правоохранными органами в угоду политической конъюнктуры, жертвуя, в то же время, интересами безопасности населения.

В случае преодоления взаимных политических претензий, эффективность противодействия экстремизму, в первую очередь, зависит от универсальности применяемых механизмов, которые

могут найти отражение в следующих правовых и организационных мерах:

- унификация антиэкстремистского и антитеррористического законодательства действующих совместно государств;
- повышение эффективности существующих, а при необходимости создание международных формирований правоохранительных органов в сфере противодействия экстремизму и терроризму;
- постоянный совместный мониторинг со стороны правоохранительных органов ситуации в сфере преступности данного вида;
- совместные действия по повышению профессионализма и обучения сотрудников правоохранительных органов в сфере противодействия экстремизму и терроризму.

В современных условиях невозможно победить международный экстремизм силами одной страны. Особенно, когда границы в мире фактически открыты. Приведенный в статье перечень возможностей, направлений и инициатив международного сотрудничества Российской Федерации в борьбе с терроризмом не претендует на исчерпывающую полноту и не может отразить всей проблематики данного вопроса. Тем не менее, следует отметить, что борьба с терроризмом по-прежнему остается важным направлением Российской внешней политики, что накладывает свой отпечаток на

⁵ Алтаева Е. Б. Экстремизм: эволюция и современные угрозы // Вопросы

национальных и федеративных отношений. 2020. Т. 10, № 5 (62). С. 1242.

характер международного
сотрудничества правоохранительных
органов в борьбе с экстремизмом.

Список литературы

1. Алтаева Е. Б. Экстремизм: эволюция и современные угрозы // Вопросы национальных и федеративных отношений. 2020. Т. 10, № 5 (62).
2. Карими Х. Х. Правовые вопросы взаимодействия в области уголовного преследования // Наука как движущая антикризисная сила: инновационные преобразования, приоритетные направления и тенденции развития фундаментальных и прикладных научных исследований: сборник научных статей по итогам международной научно-практической конференции. 2016.
3. Мухтаров М. М. Использование социальных сетей для выявления лиц, причастных к экстремистской деятельности / М. М. Мухтаров, У. Е. Ергенбек // Эффективное государство: достижения и новые направления развития: сборник научных трудов по материалам I Международной научно-практической конференции. 2017.
4. Сералиев А. Б. Правовое обеспечение противостояния терроризму и экстремизму: концептуальные подходы формирования национального законодательства // Четвертые юридические чтения. Сборник статей. 2017.
5. Шхагапсоев З. Л. Об актуальных вопросах международного сотрудничества в противодействии проявлениям экстремизма и терроризма в интернет-пространстве / З. Л. Шхагапсоев, Л. А. Бураева // Пробелы в российском законодательстве. 2018. № 5.

Dmitry N. Sudarikov

Graduate student,

Povolzhie Law Institute of The All-Russian State University of Justice

(RLA of the Ministry of Justice of Russia)

(Saratov, Russian Federation)

sudarikovfssp64@yandex.ru

Scientific supervisor – K. I. Bogomolova, PhD (Law)

PROBLEMS OF INTERNATIONAL COOPERATION OF LAW ENFORCEMENT BODIES IN COMBATING EXTREMISM AND WAYS OF THEIR SOLUTION

Abstract: This article examines the current state and problems of international cooperation of law enforcement agencies in the fight against extremism as a deterrent in countering extremist crimes. The interaction of the Russian Federation with foreign states, international and regional organizations in the field of countering extremism is analyzed, and the main ways of solving existing problems are being developed.

Keywords: extremism, international cooperation, anti-terrorist cooperation, terrorism, the fight against terrorism, law enforcement agencies, international cooperation of law enforcement agencies.

Раздел VI

ЭЛЕКТРОННОЕ ПРАВОСУДИЕ, ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Бурдина Елена Владимировна

Доктор юридических наук, доцент, заведующий кафедрой организации судебной
и правоохранительной деятельности,
Российский государственный университет правосудия
(г. Москва, Российская Федерация)
elenburdina@yandex.ru

ЦИФРОВИЗАЦИЯ СУДОВ И СПРАВЕДЛИВОСТЬ СУДЕБНОГО РАЗБИРАТЕЛЬСТВА: В ПОИСКАХ БАЛАНСА*

Аннотация: Статья посвящена проблеме поиска согласованности и баланса между цифровизацией судебной деятельности и принципами правосудия. В работе аргументируется положение о том, что независимость и самостоятельность судебной власти в современных условиях может быть достигнута только в рамках судебной системы, которая организована как доступная цифровая функция для заинтересованных лиц и действует эффективно и прозрачно.

Ключевые слова: судебная система, цифровизация судебной деятельности, цифровое правосудие, технологии, справедливость, баланс.

Для цитирования:

Бурдина Е. В. Цифровизация судов и справедливость судебного разбирательства: в поисках баланса // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 254–261.

Цифровизация как современный и объективно безальтернативный тренд развития общества и государства обусловила обсуждение вопросов внедрения IT-технологий в деятельность судов как на

международном, так и национальном уровне¹.

Проблемную повестку дня по преимуществу составляют вопросы использования систем искусственного интеллекта в деятельности судов, перевода традиционных судебных

*Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-011-00672.

¹ См., напр., выступление Гурбанова Р., президента Европейской комиссии по эффективности правосудия, на Онлайн-конференции Министров юстиции – членов Совета Европы «Независимость правосудия и верховенство закона» 9 ноября 2020 г. URL: <https://rm.coe.int/speech-ramin-opening-conf-min-justice/1680a04f41>; Котлярова В. В. К вопросу о цифровизации процесса отправления правосудия // Арбитражный и гражданский процесс. 2019. № 12. С. 46–49; Харитонов Ю. С. Платформизация правосудия: опыт Китая и будущее судебных систем мира // Вестник арбитражной практики. 2020. № 3. С. 3–11; Борисова Л. В. Об основных направлениях становления и развития электронного правосудия в современной России // Право и цифровая экономика. 2020. № 2. С. 32–35.

процессов в онлайн формат, дематериализации судебного судопроизводства, использования электронных доказательств, электронного доступа к суду и другие вопросы.

Современное развитие технологий позволяет решать многие проблемы, накопленные в судебной системе, включая чрезмерную загруженность судов и их стабильную недофинансированность. Однако у технологизации судов есть вполне очевидные риски, связанные с нивелированием принципов правосудия, вплоть до умаления отдельных из них.

В силу масштабов, глубины и скорости технологической модернизации судебной деятельности процессы цифровизации системы правосудия могут породить революционные, качественные изменения институциональных и функциональных характеристик судебной сферы, что угрожает предназначению судебной власти для защиты верховенства права и справедливости, ее роли в системе разделения властей.

В этой связи важными являются выявление закономерностей, определяющих развитие судов и правосудия в условиях цифровизации судебной деятельности, а также выбор сущностного дискурса в обсуждении возникающих в связи с этим проблем.

При фундаментальных изменениях, вызванных прорывным действием технологий, и их влиянии на организацию и функционирование всех государственных институтов, сам факт применения технологий разного рода в деятельность судов, по сути,

никогда не отрицается, представляет объективную необходимость, следствие общих закономерностей перехода к цифровому государству в отдельно взятой сфере государственной деятельности.

Более того, возрастающая общественная потребность в судебном решении обуславливает внедрение цифровых технологий в качестве надлежащего средства, способного предоставить доступ к правосудию в условиях информационного общества. Это особенно отчетливо проявилось во время пандемии по COVID-19, когда выполнение судами своей роли в обществе стало возможным посредством применения электронных форм судопроизводства и доступа к суду, электронных коммуникаций суда с гражданами.

Может показаться парадоксальным, но сохранение фундаментальных качеств и предназначения судебной власти в тех обстоятельствах, в которых проживает человечество, становится единственно возможным исключительно с применением цифровых технологий, посредством законодательного закрепления цифрового доступа к суду, создания судебных платформ, аккумулирующих сервисы по передаче и обмену судебной информацией, позволяющих гражданам участвовать в судебном разбирательстве дистанционно. При этом суды должны иметь достаточные ресурсы, программное обеспечение и системы видеоконференции, чтобы адаптироваться к новым вызовам и угрозам, включая социальное

дистанцирование и карантинные мероприятия².

Таким образом, независимость и самостоятельность судебной власти в современных условиях может быть достигнута только в рамках судебной системы, которая имеет достаточные ресурсы, организована как доступная цифровая функция для граждан и организаций и действует эффективно и прозрачно.

Следовательно, содержательный контекст обсуждения цифровизации судебной деятельности должен сводиться к двум основным аспектам: во-первых, к признанию необходимости перехода к цифровому правосудию как способу сохранения роли суда в новых условиях функционирования общества и удовлетворения потребностей социума; во-вторых, к выявлению рисков и угроз цифровизации по отношению к принципам надлежащего правосудия и формированию системы мероприятий и гарантий, нивелирующих названные угрозы. Смысл обсуждений, как представляется, следует сосредоточить на поиске необходимого баланса между техническими (машинными, электронными, цифровыми) формами судебной деятельности и гарантиями принципа справедливости судебного разбирательства, осуществляемого компетентным судьей. Сложности возникают при объединении в рамках судебной деятельности междисциплинарных методов, плохо

между собой сочетающихся. Речь идет, например, об объединении технических методов, нацеленных на повышение эффективности и снижение трудозатратности процессов, и способов, гарантирующих справедливое рассмотрение дела, где помимо законности от судьи ожидается проявление душевных качеств: сострадания, сочувствия, милосердия, мудрости, проницательности и др., а доступ к суду обеспечивается каждому гражданину независимо от его технических познаний, навыков работы с интернетом, имущественного положения.

Нынешний этап развития судебной системы является этапом поиска устойчивости основных судебных институтов при технологичности многих аспектов судебной деятельности.

Новый этап развития судебной ветви власти можно именовать «цифровым правосудием», под которым следует понимать структурно новый тип организации и деятельности судебной ветви власти, основанный на электронных сетях, цифровых базах, цифровых данных и обмене ими внутри системы, с гражданами и в межведомственном взаимодействии.

В юридической литературе отмечается, что признаком цифрового правосудия является переход большей части судебных коммуникаций в цифровую среду³.

² Консультативный Совет европейских судей (CCJE). Заявление президента КСЕС «Роль судей во время и после пандемии по COVID-

19: уроки и проблемы». Страсбург, 24 июня 2020 г.

³ См.: Брянцева О. В., Солдаткина О. Л. Электронное правосудие в России:

Представление о главных качественных особенностях цифрового правосудия раскрывают его признаки и принципы. Признаками цифрового правосудия являются следующие:

а. широкое использование современных цифровых технологий, интеграция уже существующих в единые системы, охватывающие как правосудную, так и обеспечительную деятельность судов, создание судебных сетей и сетевого взаимодействия, баз данных, киберфизических систем и систем искусственного интеллекта (технологический признак);

б. электронная форма судопроизводства;

в. создание новых организационных форм судебной деятельности в разных ее сферах: судоустройственной, судопроизводственной, обеспечительной, оформляющих новые способы функционирования судов при внедрении технологий (признак новых организационных форм);

г. изменение внутрисистемных и межведомственных способов документационного обеспечения, основанного на автоматизации, электронных сетях, судебных и иных цифровых базах и обмене цифровыми данными (признак нового способа документооборота);

д. дистанционная форма взаимодействия с гражданами, дистанционный доступ к суду;

е. сбалансированность внутрисистемных и публичных задач и повышение удовлетворенности граждан качеством и транспарентностью судебной защиты, доверия к суду (целевой признак).

Для характеристики концепции цифрового правосудия, задающей векторы развития судебной ветви власти в условиях информационного общества, могут быть сформулированы принципы доступа к суду и взаимодействия судов с гражданами и организациями как лицами, заинтересованными в судебной защите. К числу базовых принципов цифрового правосудия, вытекающих из более общей конструкции «цифровое государство», относятся пять положений:

1) доступ к суду цифровой по умолчанию (цифровой доступ к суду как тождественный традиционному доступу к суду; способ доступа выбирается самим лицом, обращающимся к суду за защитой нарушенного права);

2) платформенезависимость и ориентация на мобильные устройства при внедрении информационно-коммуникативных технологий (предусматривающий возможность выхода в интернет и цифровой доступ к суду с любого мобильного устройства, а не только с персонального компьютера);

3) проектирование судебных информационно-коммуникативных технологий с ориентиром на пользователя (понятность и простота в пользовании);

4) электронное дело (возможности осуществления судопроизводства в электронном виде, что предполагает в том числе удаленное ознакомление с делом, электронные обращения к суду и т. п.);

5) суд как единая технологическая платформа.

Пандемия короновирусной инфекции актуализировала вопрос о необходимости интеграции ГАС «Правосудие» и портала государственных услуг, хотя указанный вопрос начал обсуждаться еще с 2018 г.⁴ Посредством такой интеграции и запуском не позже 2022 г. суперсервиса «Правосудие онлайн» будет обеспечена не только возможность подавать любые обращения в суд, но и знакомиться с материалами дела, дистанционно участвовать с применением личных средств связи в судебных заседаниях, получать электронные уведомления.

Прототип суперсервиса был представлен в августе 2019 г. на портале госуслуг. Основная цель суперсервиса сформулирована так: «Меньше бумаг, пройденных километров и пропущенных судебных уведомлений на почте»⁵. Кроме того, оглашен основной функционал суперсервиса и его преимущества:

- суд для подачи иска определяется автоматически;

- документы и уведомления отправляются по судам и участникам процесса в электронном виде;

- доступ к документам по делу открыт онлайн всем участникам процесса;

- интерактивный помощник подскажет, как составить требования по иску, заполнить и подать электронное заявление;

- оплата госпошлины на портале;

- удаленное участие в процессе (доступ через биометрическую идентификацию)⁶.

Переход к новой модели организации и функционирования судебной власти – цифровому правосудию и наращиванию цифровой технологической базы судов ставит в число научных проблем решение вопроса о создании гарантий доступа к суду каждого, кто нуждается в судебной защите.

С усилением коммуникативных электронных взаимодействий необходимо расширять помощь гражданам в защите их прав в условиях цифровой судебной среды. Безбумажные и дистанционные технологии требуют значительных и долгосрочных затрат и усилий по общению с населением, прежде чем можно ожидать, что достаточное количество граждан узнает о наличии новых инструментов и будет ими пользоваться; произойдут изменения в

⁴ См.: Юридическая концепция роботизации: монография / Н. В. Антонова, С. Б. Бальхаева, Ж. А. Гаунова [и др.]; отв. ред. Ю. А. Тихомиров, С. Б. Нанба. М.: Проспект, 2019.

⁵ Представлены прототипы новых пяти суперсервисов // Информационно-правовой портал Гарант.ру. URL:

<https://www.garant.ru/news/1290222/> (дата обращения: 04.04.2021).

⁶ Представлены прототипы новых пяти суперсервисов // Информационно-правовой портал Гарант.ру. URL: <https://www.garant.ru/news/1290222/> (дата обращения: 04.04.2021).

культуре и поведении граждан в их взаимоотношениях с системой правосудия.

По этой причине инвестиции государства в коммуникативные технологии, повышающие эффективность судов, должны сопровождаться активной коммуникативной политикой судов, направленной на оказание помощи гражданам в новых условиях организации судебной деятельности. Такая помощь должна оказываться в разных формах: через создание новых удобных форматов работы суда, через физический прием граждан в судах, через веб-ресурсы (сайты судов), через предоставление доступа к процедурам урегулирования споров как в онлайн-режиме, так и в здании суда. Важным является создание инновационных приемных судов, где сотрудники суда могли бы оказать помощь гражданам в электронной подаче иска или другого обращения, что позволит устранить риски цифрового неравенства, достичь удобства для граждан и повысить их доверие к суду.

Многие проблемы электронного (цифрового) правосудия связаны не с характером и достаточностью правового регулирования и степенью внедрения технологий, а с вопросами рациональной судебной организации, перераспределения и распределения судебных ресурсов и финансирования, администрирования судами.

Так, недооценка факторов служебной нагрузки на суды и оценки и управления судебной нагрузкой создает угрозу реализации принципов правосудия и качеству судебных актов. Изменившиеся социально-демографические и экономические

факторы, возможности дистанционного взаимодействия с судом трансформируют представления о доступности суда, что требует новых подходов к разработке принципов построения судебной организации в условиях информационного общества и нового содержательного наполнения принципа доступа к суду.

Запрос общества в отношении новой парадигмы управления, предполагающей иные подходы к качеству управления и управленческой культуре, обусловили новые направления управления и администрирования судов, в числе которых эффективное управление ресурсами, являющееся новым, основанным на экономических подходах методом совершенствования судебной системы. Предстоит оценить как возможности, так и риски данного способа, поскольку есть опасность конфликта с обязательством судов по справедливому разбирательству дел.

Тем самым, иная технологическая основа судебной деятельности, преобразующая функционально-структурную модель судебной власти, неизбежно влечет создание новых организационных форм судебной деятельности в разных ее сферах: судоустройственной, судопроизводственной, обеспечительной.

В качестве таких новых организационных форм могут выступать: преобразование «судебных карт», что предполагает укрупнение судов вследствие развития дистанционных форм доступа к суду и возможностей участия граждан в судебных заседаниях в онлайн

форматах; создание судебных администраций и определение исключительных полномочий администратора суда; создание форм помощи гражданам в реализации их прав на обращение к суду в электронном формате; новые формы финансирования судов, основанные на показателях служебной нагрузки; организационные формы перераспределения нагрузки с чрезмерно загруженных судов в

рамках региона и судебного округа и другие.

Новые организационные формы судебной деятельности придадут устойчивость существующим судебным институтам, меняющим содержание под влиянием технологий, что, в свою очередь, позволит планомерно развивать судебную систему через реформы, а не революционным способом, путем изменяющих правосудие рывков.

Список литературы

1. Борисова Л. В. Об основных направлениях становления и развития электронного правосудия в современной России // Право и цифровая экономика. 2020. № 2. С. 32–35.
2. Брянцева О. В. Электронное правосудие в России: проблемы и пути решения / О. В. Брянцева, О. Л. Солдаткина // Вестник ун-та им. О. Е. Кутафина (МГЮА). 2019. № 12 (64). С. 97–104.
3. Котлярова В. В. К вопросу о цифровизации процесса отправления правосудия // Арбитражный и гражданский процесс. 2019. № 12. С. 46–49.
4. Харитонов Ю. С. Платформизация правосудия: опыт Китая и будущее судебных систем мира // Вестник арбитражной практики. 2020. № 3. С. 3–11.
5. Юридическая концепция роботизации : монография / Н. В. Антонова, С. Б. Бальхаева, Ж. А. Гаунова [и др.]; отв. ред. Ю. А. Тихомиров, С. Б. Нанба. М.: Проспект, 2019. 240 с.

Elena V. Burdina

Doctor of Law Doctor of Law, Associate Professor, Head of Department of
Organization of the judiciary and law enforcement,
Russian State University of Justice
(Moscow, Russian Federation)
elenburdina@yandex.ru

DIGITALIZATION OF COURTS AND FAIRNESS OF TRIAL: IN SEARCH OF A BALANCE

Abstract: The article is devoted to the problem of finding consistency and balance between the digitalization of judicial activity and the principles of justice. The paper argues the position that the independence and independence of the judiciary in modern conditions can be achieved only within the judicial system, which is organized as an accessible digital function for stakeholders and operates efficiently and transparently.

Keywords: judicial system, digitalization of judicial activity, digital justice, technology, fairness, balance.

Кукеев Аскар Кульчимбаевич

Старший преподаватель кафедры Теории государства и права,

Южно-Казахстанский Университет им. М. Ауэзова

(г. Шымкент, Республика Казахстан)

askar_kukeyev@mail.ru

КОНСТИТУЦИОННО-ПРАВОВЫЕ ОСНОВЫ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО СУДОПРОИЗВОДСТВА В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация: Статья посвящена конституционно-правовым основам использования цифровых технологий в судопроизводстве Республики Казахстан, определению направлений и способов развития и использования цифровых технологий и разработке предложений по совершенствованию законодательства в этой сфере. Современные цифровые технологии в судопроизводстве – это законодательно урегулированная единая система средств и приемов сбора, фиксации, обработки, хранения и распространения правовой информации, а также создания документов и их проектов в электронной форме с помощью компьютерной техники, интернет-приложений, автоматизированных систем, информационно-коммуникационных сетей и других цифровых средств, организованная на всех уровнях и во всех основных сферах общественного управления, других видах юридической деятельности, которая позволяет повысить эффективность соответствующей деятельности.

Также определено, что электронное судопроизводство (правосудие) – это единая, целостная и комплексная информационно-телекоммуникационная система, интегрированная в деятельность судов, других субъектов, которые наделены полномочиями, связанными с обеспечением правосудия, посредством применения цифровых технологий, состоящих из отдельных элементов, которые могут функционировать как самостоятельно, так и в системе с другими.

Ключевые слова: судебная система, суд, участники судебного процесса, электронный суд, электронный кабинет, электронная подпись, официальная электронная почта, информационно-коммуникационные технологии.

Для цитирования:

Кукеев А. К. Конституционно-правовые основы организации электронного судопроизводства в Республике Казахстан // Технологии XXI века в юриспруденции: материалы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 262–272.

В соответствии со ст. 77 Конституции Республики Казахстан¹ и статьями. 1–2 Конституционного закона Республики Казахстан «О судебной системе и статусе судей Республики Казахстан»², основными принципами судопроизводства являются: законность; равенство всех перед законом и судом; гласность судебного процесса и его полная цифровизация техническими средствами; разумные сроки рассмотрения дела судом; доступность правосудия для каждого лица и тому подобное. Ряд международных актов также закрепляет основополагающие требования и стандарты обеспечения доступности, эффективности, информационной прозрачности правосудия³.

В значительной степени обеспечению реализации международных и национальных основ судопроизводства способствует введение в Республике Казахстан электронного судопроизводства (правосудия), которое является одним из направлений применения цифровых технологий в праве и одним из элементов системы электронного управления. Вместе с тем система электронного судопроизводства

(правосудия) характеризуется определенным уровнем обособленности от других элементов электронного управления, что обусловлено независимостью судебной власти и ее особым правовым статусом в системе разделения государственной власти.

Внедрение и обеспечение надлежащего функционирования системы электронного судопроизводства (правосудия) является потребностью информационного общества, обычной требованию настоящего, которая сейчас является неотъемлемой от понятий «справедливое», «эффективное» и «доступное» правосудия.

Некоторые зарубежные ученые по этому поводу отмечают, что электронное правосудие является жизненно важной политикой и столь же важным инструментом для модернизации и улучшения предоставления правосудия в Европе, то ли на национальном, или на наднациональном или трансграничном уровне⁴.

Важность и необходимость ускорения процесса внедрения системы электронного судопроизводства (правосудия) в

¹ Конституция Республики Казахстан (принята 30 августа 1995 года на республиканском референдуме) // ИПС «ӘДІЛЕТ». URL: https://adilet.zan.kz/rus/docs/K950001000_ (дата обращения: 26.04.2021).

² О судебной системе и статусе судей Республики Казахстан: Конституционный закон Республики Казахстан от 25 декабря 2000 года № 132 // ИПС «ӘДІЛЕТ». URL: https://adilet.zan.kz/rus/docs/Z000000132_ (дата обращения: 26.04.2021).

³ Гришин Д. А. Международные стандарты уголовного судопроизводства // Юридическая наука и правоохранительная практика. 2020. № 1 (51). С.67–68.

⁴ Xanthoulis N. Introducing the concept of «E-justice» in Europe: How adding an «E» becomes a modern challenge for Greece and the EU // Effectivt, justice, solutions. 2010. URL: http://effectivt.com/yahoo_site_admin/assets/docs/Introducing_the_concept_of_e-justice_in_Europe_by_Napoleon_Xanthoulis.20775004.pdf (accessed: 26.04.2021).

Украине неоднократно подчеркивали отечественные ученые. Так, Д. М. Усабаева отметила, что сегодня гражданское общество уже не может существовать без цифровых технологий. Поэтому благодаря индустриальной революции Украина имеет возможность стать одной из ведущих стран в сфере развития цифровых технологий, для чего необходимо создать благоприятные условия для этого, то есть осуществлять реорганизацию или замену как систем административно-организационной поддержки судов, так и компьютеризированных систем юридической информации⁵.

Международными институтами по этому поводу отмечается, что доступ к правосудию для всех является частью обеспечения справедливости в обществе. Обеспечение этого права стало одной из задач, определенных Европейской хартией этики об использовании искусственного интеллекта в судебных системах и их окружении⁶, в которой отмечается, что использование информационных технологий и инструментов в судебных системах имеет целью повышение эффективности и качества правосудия, и их следует поощрять. Однако это должно осуществляться ответственно, при соблюдении основных прав людей, закрепленных Европейской конвенцией о правах

человека и Конвенцией о защите персональных данных, и в соответствии со следующими принципами:

1) применение цифровых технологий и инструментов, основанных на их использовании, в судопроизводстве должно быть совместимо с основными правами человека;

2) предотвращение развития или усиления любой дискриминации между отдельными лицами или группами лиц при применении соответствующих инструментов;

3) осуществление обработки судебных решений и судебных данных с использованием только сертифицированных и безопасных механизмов;

4) обеспечение безопасной технологической среды для хранения судебных данных в информационных системах;

5) применение допустимых и понятных методов обработки судебных данных с возможностью проведения внешнего аудита таких методов.

Таким образом, по нашему мнению, введение электронного судопроизводства является важным в контексте повышения доступа к правосудию, поскольку доступность – это не только физический доступ в суд, а для эффективного решения правовых проблем граждане требуют

⁵ Усабаева Д. М. Вопросы электронного правосудия в Республике Казахстан // Закон.кз. URL: <https://www.zakon.kz/4889459-voprosy-elektronnogo-pravosudiya-v.html> (дата обращения: 01.05.2021).

⁶ Европейская этическая хартия об использовании искусственного интеллекта в

судебных системах и окружающих их реалиях. Принята на 31-м пленарном заседании ЕКЭП (Страсбург, 3–4 декабря 2018 года) // СПС «Параграф Online» https://online.zakon.kz/Document/?doc_id=35417997 (дата обращения: 25.04.2021).

быстрого и удобного доступа к судебным услуг не только в здании суда. А судам для этого необходимо иметь эффективные электронные инструменты управления прохождением дел. Поэтому значительное внимание, которое уделяется вопросу внедрения и распространения цифровых технологий в сферу судопроизводства, свидетельствует об актуальности и важности данного вопроса для дальнейшего развития судебной системы.

Определенные шаги на пути интеграции цифровых технологий в сферу судопроизводства сделано и в Республике Казахстан. Так, Стратегия информационно-коммуникационных технологий для судебной системы РК⁷ среди стратегических вопросов, решение которых имеет приоритетное значение для развития судебной системы, определяет такие как обеспечение доступа к правосудию и использование инновационных технологий и улучшения судебного процесса.

Кроме того, создание специального программного продукта для налаживания работы в соответствии с современными требованиями в период пандемии COVID-19 является крайне необходимым, поскольку сегодня вся работа по осуществлению правового поиска и анализа имеющихся правовых позиций выполняется судьей самостоятельно, в ручном

режиме, что значительно влияет на качество судебных решений.

Таким образом, не вызывает сомнений тот факт, что введение системы электронного судопроизводства (правосудия) является настоящим вызовом, потребностью дальнейшего развития судебной системы, обеспечение эффективности осуществления судопроизводства в информационном обществе.

В национальной судебной системе результатом внедрения технологий в судопроизводство является создание и полноценное функционирование Автоматизированной информационно-аналитической системы судебных органов РК «Төрелік», задача которой состоит в обеспечении пользователя путем оперативного доступа к обмену информационными данными. Данная программ имеет высокую степень надежности и решает такие задачи как ведение автоматизированной системы учета и контроля соблюдения процессуальных сроков, наличие статистических и аналитических отчетов, упрощение делопроизводства и судопроизводства.

Автоматизированная информационно-аналитическая система судебных органов РК «Төрелік», включает в себя следующие системы:

- 1) Судебное делопроизводство и документооборот;
- 2) Распределение судебных

⁷ Стратегия информационно-коммуникационных технологий для судебной системы РК от 28.05.2020 // Сайт Верховного Суда РК. URL:

<https://www.sud.gov.kz/rus/content/informacionnye-tehnologii-v-sovremennyh-sudah-kazahstana> (дата обращения: 24.04.2021).

дел;

- 3) Судебная статистика;
- 4) Судебная практика;
- 5) Электронная библиотека суда;
- 6) Кадры;
- 7) Аналитика;
- 8) Материально-техническое обеспечение;
- 9) Законодательство и право;
- 10) Протоколирование и звукозапись судебного процесса;
- 11) Видео-конференц-связь;
- 12) Единый государственный реестр судебных решений и др.

Таким образом, можно сделать вывод, что система электронного судопроизводства (правосудия) состоит из элементов, которые условно следует разделить на три группы:

- 1) те, которые обеспечивают взаимодействие суда и участников судебного процесса (электронный суд), то есть направлены непосредственно на осуществление судопроизводства и связанных с ним процессов (подача искового заявления, апелляционной, кассационной жалоб в электронной форме, отслеживание хода рассмотрения дела в сети Интернет, направление судебных повесток, сообщений средствами электронной связи, участие в рассмотрении дела в режиме видеоконференции, доступе к судебным решениям и т. п.);

- 2) те, которые обеспечивают взаимодействие судов между собой, а также суда с другими органами публичного управления (система

электронного документооборота, доступ в государственные реестры, получения и проверка подлинности электронных доказательств и т. п.);

- 3) те, которые обеспечивают организацию внутренних управленческих процессов (электронная система анализа судебной практики, электронная система судебной статистики, электронные архивы, электронная библиотека суда и т. п.).

Вместе с тем некоторые ученые отмечают, что система электронного судопроизводства в перспективе может значительно расширить свои возможности, в частности обеспечить автоматизацию самого процесса принятия некоторых видов судебных решений. К примеру, в Аргентине в 2017 было апробировано программное приложение Prometea, с помощью которого возможно примерно за 10 секунд вынести и оформить судебное решение по ряду категорий гражданских и административных дел. В ходе мониторинга результатов работы указанного приложения оказалось, что местными судьями были подтверждены 100 % таких решений, принятых за последний год с помощью такого приложения⁸.

Указанное свидетельствует о том, что большинство видов аналитической деятельности, основанной на многократном повторении подобных операций с применением определенной системы алгоритмов и/или не требующей нестандартного (творческого, креативного) подхода, могут быть

⁸ Иванов М. Решения робота-судьи полностью устраивают служителей Фемиды // Legal Report. 2018. URL:

<https://legal.report/resheniya-robota-sudii-polnostyu-ustraiwayut-sluzhitelej-femidy/> (дата обращения: 24.04.2021).

автоматизированы с помощью новейших технологий. Не является исключением и деятельность, связанная с осуществлением правосудия. Вместе с тем необходимо учитывать, что современные цифровые технологии хотя и значительно облегчают (автоматизируют) процесс реализации некоторых функций судопроизводства, однако полностью заменить человека в такой сфере деятельности, как юриспруденция, не могут, что связано с исключительной способностью человека к применению творческого подхода, умением находить нестандартные пути решения сложных вопросов, на которые искусственный интеллект не способен.

Итак, система электронного судопроизводства предоставляет ряд возможностей и преимуществ по сравнению с традиционной системой судопроизводства, которые выражаются, прежде всего:

1) для участников судебного процесса в возможности: подавать заявления и жалобы, иные процессуальные документы в электронной форме, то есть из любого места, где есть техническая возможность и доступ к ПК и Интернету, принимать участие в судебном процессе в режиме видеоконференции, отслеживать движение дела по WEB-ресурсам судебной власти, платить судебный сбор с помощью системы электронных платежей, получать и направлять в суд процессуальные документы с помощью средств электронной связи, иметь доступ к судебным решениям в соответствующих реестрах, подавать в

суд доказательства в электронной форме и тому подобное;

2) для судей в возможности: иметь доступ к нормативно-правовым актам, судебной практике, аналитическим материалам, автоматизировать некоторые мониторинговые процессы по анализу судебной практики и актов законодательства, получать и проверять подлинность доказательств в электронной форме, проверять информацию, содержащуюся в государственных реестрах, подписывать судебные решения с помощью цифровой подписи и т. д.;

3) для работников аппарата судов и органов обеспечения системы правосудия в возможности: автоматизации некоторых управленческих процессов (статистическая отчетность и т. п.), формировании судебных дел, процессуальных документов в электронной форме, осуществления электронного документооборота не только в пределах суда, но и с другими органами публичного управления, участниками судебного процесса и т. д.

Кроме того, внедрение системы электронного судопроизводства способствует существенной экономии средств государственного бюджета и частных лиц, упрощению и ускорению судебного разбирательства, автоматизации и стандартизации процессов делопроизводства в суде и повышению качества отправления правосудия.

Однако, несмотря на существенные преимущества системы электронного судопроизводства, большинство ученых обращают

внимание на определенные риски и проблемные моменты, возникающие (или которые могут возникнуть) в процессе внедрения цифровых технологий в судопроизводство. К примеру, Р. К. Сарпекоев указывает на достаточно высокий риск потери юридически важной информации, отсутствие «компьютерной грамотности» на уровне квалифицированных пользователей у судей и сотрудников аппарата судов (что представляет серьезную проблему для людей особенно старшего поколения), сложность разработки и ввода в эксплуатацию (что в наших условиях еще более сложное дело) соответствующего программного обеспечения; требуемое техническое оснащение судов⁹.

Указанное мнение поддерживают и другие ученые, которые считают, что введение электронного правосудия ставит больше вопросов, чем дает ответов. В частности, Г. А. Абрамович отмечает, что помимо проблемы защищенности системы, появляется вопрос по хранению значительных баз данных и возможности доступа к ним с течением времени. Особенно остро данный вопрос, как считает ученый, возникает в контексте того, кто именно будет распорядителем указанных баз данных, а также как будет обеспечиваться защита не только от постороннего

вмешательства, но и от возможного злоупотребления правами собственно распорядителем, поскольку информация, предоставляемая суду и сохраняемая в электронной системе, может относиться к коммерческой тайне, то есть возникают серьезные угрозы защищенности такой информации¹⁰.

Действительно, проблема обеспечения информационной безопасности непосредственно связана с регулированием вопроса определения владельцев (распорядителей) информационно-телекоммуникационной системы, в которой хранится соответствующая информация, то есть определение и осуществление контроля за состоянием информационной безопасности. Так, согласно Закону Республики Казахстан «О персональных данных и их защите»¹¹ субъекты публично-властных полномочий принимают соответствующие подзаконные акты, в которых определяют порядок, особенности защиты информации, распорядителями, владельцами или пользователями которой являются указанные субъекты. На данный момент подобного нормативного акта, в котором бы определялись основы защиты информации в Автоматизированной информационно-аналитической системе судебных органов РК «Төрелік», не разработано.

⁹ Сарпекоев Р. К. Цифровизация правового пространства // Вестник Института законодательства и правовой информации Республики Казахстан. 2020. № 3 (61). С. 18.

¹⁰ Абрамович Р. Практические аспекты внедрения электронного правосудия в

Украине // Юридическая газета. 2017. № 46. С. 15.

¹¹ О персональных данных и их защите: закон Республики Казахстан от 21 мая 2013 года № 94-V // Казахстанская правда. 2013. 25 мая. № 178-179.

Вместе с тем видится необходимым дополнить Уголовный кодекс Республики Казахстан¹² статьей, предусматривающей уголовную ответственность за незаконное вмешательство в работу автоматизированной системы документооборота суда, таким образом уголовная ответственность будет применяться за незаконное вмешательство в работу автоматизированных систем в органах и учреждениях системы правосудия.

Итак, ожидаемые риски и проблемы, обусловленные внедрением системы электронного судопроизводства, должны быть предусмотрены и максимально минимизированы еще на этапе планирования внедрения системы и на этапе ее функционирования в тестовом режиме, в том числе путем осуществления соответствующих правовых (принятие нормативно-правовых актов о мерах информационной безопасности, порядке работы отдельных элементов системы и т. д.), организационных (определение механизма функционирования определенных элементов системы), информационных (определение потребностей, на удовлетворение которых направлено действие отдельных элементов системы и их взаимоувязки) мероприятий. Однако бесспорным является то, что любые риски не могут и не должны тормозить процесс внедрения цифровых технологий в деятельность судебной власти, поскольку преимущества от

внедрения системы электронного судопроизводства абсолютно преобладают над возможными рисками и временными трудностями переходного этапа.

Так, например, возникает вопрос о порядке принятия доказательств, поскольку электронный суд будет принимать доказательства только в электронной форме. Во-первых, возникает проблема со значительными объемами документов, которые, возможно, потребуют сканирования. Второй проблемой является проблема подделки, поскольку подделать документ с помощью графических и текстовых редакторов может большинство компьютерных пользователей, и так возникает связанная с этим проблема проверки судом подлинности представленных доказательств.

Выводы:

1. Электронный суд является элементом электронного судопроизводства, в рамках которого обеспечиваются рассмотрение и решение судебного дела с помощью соответствующих информационных технологий. Введение в Казахстане электронного судопроизводства, которое является одним из направлений применения цифровых технологий в праве и одним из элементов системы электронного управления, в значительной мере способствует обеспечению реализации международных и национальных принципов судопроизводства. Вместе с тем

¹² Уголовный кодекс Республики Казахстан: кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК // ИПС «ӘДІЛЕТ». URL:

<https://adilet.zan.kz/rus/docs/K1400000226/info> (дата обращения: 24.04.2021).

система электронного судопроизводства характеризуется определенным уровнем обособленности от других элементов электронного управления, что обусловлено независимостью судебной власти и ее особым правовым статусом в системе разделения государственной власти.

2. Преимуществами системы электронного судопроизводства являются:

а) Открытость деятельности в сфере осуществления правосудия, которая выражается в создании условий для свободного доступа каждого человека к судебным решениям, информации о суде и судьях, других участниках судебного процесса, графике рассмотрения дел и другой информации, дает возможность осуществлять общественный контроль над деятельностью судебной власти, проводить мониторинг судебных решений. Как результат, внедрение электронного судопроизводства является одним из инструментов предотвращения коррупции в судебной системе и усложняет возможность избежать ответственности за принятие неправосудных решений.

б) Оперативность и экономия ресурсов, что обусловлено автоматизацией некоторых процессов в ходе рассмотрения и разрешения дела (экономия времени), уменьшением расходов на пересылку судебной корреспонденции и расходов на оформление судебных решений в бумажной форме (экономия средств) и др.

в) Удобство и повышение

доступности правосудия предусматривает возможность обращения в суд, принятие участия в рассмотрении дела, оплаты судебного сбора, получения судебного решения в электронной форме (как оригинала) в любое время и из любого места при наличии соответствующих технических возможностей и доступа к сети Интернет.

г) Точность информации, содержащейся в процессуальных документах, возможность избежать технических, статистических, арифметических и других ошибок при их формировании и тому подобное.

3. Факторами, которые замедляют процесс внедрения системы электронного судопроизводства, являются:

- 1) организационная, правовая, материально-техническая неготовность к внедрению всех элементов системы электронного (отсутствие надлежащего компьютерного и программного обеспечения);
- 2) недостаточная унифицированность информационного пространства органов судебной власти, других органов публичного управления (несовместимость различных элементов системы, отсутствие единых стандартизированных форм шаблонов документов и т. п.);
- 3) неполный учет ключевых потребностей пользователей системы (судей, участников судебного процесса, работников аппарата судов и других органов обеспечения деятельности органов правосудия), то есть недостаточная функциональная способность некоторых подсистем. Угрозами и рисками, вызванными

функционированием системы электронного судопроизводства, являются: 1) риск несанкционированной утечки информации в Единой судебной информационно-телекоммуникационной системе или несанкционированного вмешательства в работу системы; 2) зависимость системы от бесперебойной работы электросети, сети Интернет, компьютерного оборудования и программ; 3) зависимость системы от законодательных изменений и невозможность оперативной доработки уже функционирующей системы в случае поспешности внесения таких изменений.

4. Дальнейшее развитие системы электронного судопроизводства, в том числе с учетом зарубежного опыта в этой сфере, должно осуществляться в следующих направлениях: 1) необходим переходный этап, во время которого будут функционировать параллельно

система электронного и традиционного правосудия (в отношении тех элементов, которые на данный момент не внедрены в полной мере) постепенный переход к обязательной системе электронного судопроизводства по мере готовности как самой системы к эксплуатации, так и пользователей: проведение постоянного мониторинга потребностей пользователей системы, ранжирование проблем, возникающих в ходе ее эксплуатации и т. д.; 2) применение комплексного подхода к внедрению системы электронного судопроизводства, в частности путем обеспечения совместимости и связанности различных элементов этой системы между собой и с другими элементами электронного управления; 3) принятие нормативно-правовых актов о мерах обеспечения информационной безопасности, в частности о защите информации в Единой судебной информационно-телекоммуникационной системе.

Список литературы

1. Абрамович Р. Практические аспекты внедрения электронного правосудия в Украине // Юридическая газета. 2017. № 46. С. 14–15.
2. Гришин Д. А. Международные стандарты уголовного судопроизводства // Юридическая наука и правоохранительная практика. 2020. № 1 (51). С. 65–74.
3. Иванов М. Решения робота-судьи полностью устраивают служащих Фемиды // Legal Report. 2018. URL: <https://legal.report/resheniya-robota-sudi-polnostyu-ustraiyut-sluzhitelej-femidy/>.
4. Сарпекоев Р. К. Цифровизация правового пространства // Вестник Института законодательства и правовой информации Республики Казахстан. 2020. № 3 (61). С. 12–24.
5. Усабаева Д. М. Вопросы электронного правосудия в Республике Казахстан // Закон.кз. URL: <https://www.zakon.kz/4889459-voprosy-elektronnogo-pravosudiya-v.html>.

6. Xanthoulis N. Introducing the concept of «E-justice» in Europe: How adding an «E» becomes a modern challenge for Greece and the EU // Effectivt, justice, solutions. 2010. URL: http://effectius.com/yahoo_site_admin/assets/docs/Introducing_the_concept_of_e-justice_in_Europe_by_Napoleon_Xanthoulis.20775004.pdf.

Askar K. Kukeyev

Senior Lecturer, Department of Theory of State and Law,
South Kazakhstan University named after M. Auezov
(Shymkent, Republic of Kazakhstan)
askar_kukeyev@mail.ru

CONSTITUTIONAL AND LEGAL BASES OF THE ORGANIZATION OF ELECTRONIC LEGAL PROCEEDINGS IN THE REPUBLIC OF KAZAKHSTAN

Abstract: The article is devoted to the constitutional and legal bases of the use of digital technologies in the judicial proceedings of the Republic of Kazakhstan, the definition of directions and methods of development and use of digital technologies and the development of proposals for improving legislation in this area. Modern digital technologies in legal proceedings are a legally regulated unified system of means and techniques for collecting, recording, processing, storing and distributing legal information, as well as the creation of documents and their drafts in electronic form using computer technology, Internet applications, automated systems, information and communication networks and other digital means, organized at all levels and in all major areas of public administration, other types of legal activity, which allows to increase the efficiency of relevant activities.

It is also defined that electronic judicial proceedings (justice) is a single, integral and complex information and telecommunications system integrated into the activities of courts and other entities that are empowered to ensure justice through the use of digital technologies, consisting of separate elements that can function both independently and in a system with others.

Keywords: judicial system, court, participants in the trial, electronic court, electronic cabinet, electronic signature, official e-mail, information and communication technologies.

УДК 651.004

Белошицкая Екатерина Вячеславовна
Помощник судьи Петроградского районного суда
города Санкт-Петербурга
(г. Санкт-Петербург, Российская Федерация)
beloshickaya-eka@mail.ru

ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ В СУДАХ ОБЩЕЙ ЮРИСДИКЦИИ

Аннотация: В статье характеризуется состояние электронного правосудия в российском государстве, делая акцент на таком его элементе, как электронный документооборот в судах общей юрисдикции. Используется обширная нормативная правовая база, анализируются основные направления электронного документооборота, выявляются связанные с ним проблемы и предлагаются пути их решения.

Ключевые слова: электронное правосудие, гражданский процесс, административный процесс, уголовный процесс, электронный документ, документ в электронном виде, судебный акт.

Для цитирования:

Белошицкая Е. В. Электронный документооборот в судах общей юрисдикции // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 273–278.

Вопрос электронного документооборота в судах общей юрисдикции – это, прежде всего, вопрос электронного правосудия. Согласно Концепции развития информатизации судов до 2020 г., электронное правосудие понимается одновременно в качестве способа и формы осуществления процессуальных действий в порядке использования информационных технологий, причем акцент делается на взаимодействии субъектов процессуальных отношений в электронной форме¹. При этом,

наличие легального определения электронного правосудия никак не сказывается на масштабах дискуссионности данного понятия в отечественной правовой науке. Анализ научных публикаций 2016–2021 гг., раскрывающих вопросы электронного правосудия, позволил выявить следующие определения рассматриваемого правового явления:

1. способ и форма осуществления процессуальных

¹ Концепция развития информатизации судов до 2020 г. // СПС «Гарант». URL:

<http://base.garant.ru/71062432/>
(дата обращения: 10.05.2021).

(дата

действий посредством информационных технологий²;

2. переход от бумажного к электронному документообороту, электронному взаимодействию субъектов процессуальных отношений³;

3. возможность суда и других субъектов процессуальных отношений совершать процессуальные действия, оказывающие влияние на исход судебного разбирательства, в электронной форме⁴;

4. способ осуществления правосудия, базирующийся на использовании современных информационно-коммуникационных технологий и преследующий цель обеспечения основных принципов судопроизводства⁵;

5. фактически электронный порядок документооборота правосудия и т. д.⁶

Данные определения электронного правосудия обладают некоторыми общими признаками, к числу которых можно отнести, прежде всего, осуществление процессуальных действий посредством использования информационных технологий. Кроме того, рассмотренные определения

фактически ставят вопрос о том, какое место в системе электронного правосудия занимает электронный документооборот, так как во всех из них речь идет о взаимодействиях субъектов процессуальных отношений, которое, как правило, предполагает именно документооборот.

Стоит заметить, что понятие электронного правосудия фактически отождествляется с понятием электронного суда, электронного судопроизводства. Данные понятия действительно обладают некоторыми общими чертами, обусловленными тем, что оба они базируются на информационных системах, информационном взаимодействии. Однако электронный суд, как отмечает И. В. Воронцова, мнение которой представляется верным, все же является более узким по смыслу понятием, подразумевая преимущественно электронный документооборот (направление исковых заявлений в электронном виде, участие в судебном заседании посредством системы видеоконференцсвязи и т. д.)⁷.

Соотношение электронного правосудия и электронного

² Семушин А. В. Электронное правосудие в России – этапы и механизмы реализации // Современные тенденции развития гражданского и гражданского процессуального законодательства и практики его применения. 2017. С. 368.

³ Гордиенко Е. Л. Электронное правосудие: генезис и перспективы // Научные горизонты. 2019. № 5-1 (21). С. 133.

⁴ Борисова Л. В. Электронное правосудие как форма судебной защиты в России // Актуальные проблемы российского права. 2020. Т. 15, № 6 (115). С. 106.

⁵ Брянцева О. В., Солдаткина О. Л. Электронное правосудие в России: проблемы и пути решения // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 12 (64). С. 98.

⁶ Трофимов Я. В. Сущность понятия «электронное правосудие» в процессуально-правовой доктрине // Форум. Серия: Гуманитарные и экономические науки. 2020. № 3 (20). С. 39.

⁷ Воронцова И. В. О соотношении понятий «электронный суд» и «электронное правосудие» // Правовая политика и правовая жизнь. 2019. № 3. С. 168.

документооборота характеризуют также Д. Х. Валеев и А. Г. Нуриев, приводящие следующие критерии разграничения рассматриваемых понятий. Во-первых, уровень правового регулирования, поскольку электронное правосудие регламентируется на уровне законодательных актов, а электронный документооборот – на уровне подзаконных актов. Во-вторых, субъект использования, поскольку электронное правосудие реализуется судом, а в электронном документообороте преимущественно участвуют сотрудники аппарата суда⁸. Стоит заметить, что второй критерий представляется несколько сомнительным, поскольку участниками электронного документооборота могут являться стороны спора, их представители и т. д.

Соответственно, на основе анализа научных исследований 2016–2021 гг. удалось установить, что электронное правосудие и электронный документооборот соотносятся как общее и частное, хотя последний и составляет значительную часть электронного правосудия на практике. Так, например, с 2006 г.

успешно функционирует система «ГАС Правосудие», в рамках которой существует возможность подавать процессуальные документы в электронном виде, осуществлять поиск по делам и судебным актам и т. д. Кроме того, с 2017 г. у судов имеется возможность оформлять судебные акты в электронной форме, используя при этом усиленную квалифицированную электронную подпись, что также является важным фактором совершенствования электронного документооборота в судах общей юрисдикции.

Изготовление судами судебных актов в электронной форме представляет собой одновременно и элемент электронного правосудия, и элемент электронного документооборота как его части. Возможность и специфика порядка изготовления таких судебных актов устанавливается в отраслевых процессуальных кодексах, включая ч. 1 ст. 13 ГПК РФ, ч. 1.1 ст. 16 КАС РФ и ч. 2 ст. 474.1 УПК РФ⁹. Кроме того, отдельные аспекты изготовления таких судебных актов проясняются в п. 26 Постановления Пленума Верховного Суда РФ от 26.12.2017 № 57¹⁰. Данные документы содержат

⁸ Валеев Д. Х., Нуриев А. Г. Электронный документооборот в сфере правосудия в условиях цифровой экономики // Вестник Пермского университета. Юридические науки. 2019. № 45. С. 29.

⁹ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 08.12.2020) // Собрание законодательства РФ. 2001. № 52. Ст. 4921; Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 08.12.2020, с изм. от 12.01.2021) // Собрание законодательства РФ. 2002. №

46. Ст. 4532; Кодекс административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ (ред. от 08.12.2020) // Собрание законодательства РФ. 2015. № 10. Ст. 1391.

¹⁰ Постановление Пленума Верховного Суда РФ от 26.12.2017 № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов» // СПС «Гарант». URL: <http://base.garant.ru/71844996/> (дата обращения: 10.05.2021).

ключевое положение: судебные акты, за исключением актов, содержащих сведения, составляющие охраняемую законом тайну, могут быть изготовлены в форме электронного документа, подписанного судьей усиленной квалифицированной электронной подписью.

Кроме того, указанные документы, в особенности Постановления Пленума Верховного Суда РФ от 26.12.2017 № 57, регламентируют особенности обращения судебных актов в форме электронных документов, т. е. собственно электронный документооборот. Особое внимание в указанных документах уделяется таким вопросам, как разграничение случаев направления судебного акта в форме электронного документа и в форме заверенного электронного образа бумажного документа, установление перечня лиц, обладающих правом на получение судебных актов в форме электронного документа, и т. д. Акцентируется в данных документах внимание и на такой стороне обращения судебных актов, как публикация текстов судебных решений в сети Интернет.

Тем не менее, несмотря на кажущуюся достаточность нормативной базы в данной сфере, существуют в рамках правового регулирования электронного документооборота в судах и некоторые проблемы. В частности, согласно п. 5 ч. 1 ст. 378 ГПК РФ, подаваемая на судебный акт жалоба в обязательном порядке должна сопровождаться обжалуемым актом, что может толковаться судами как обязанность заявителя, который в

таком случае должен будет распечатать и соответствующим образом заверить судебный акт. Такое толкование судами нормы п. 5 ч. 1 ст. 378 ГПК РФ способно негативно сказаться на обеспечении прав и законных интересов заявителей, поскольку указанные манипуляции с электронным судебным актом неизбежно повлекут за собой временные и финансовые затраты. Поэтому целесообразным представляется внесение в данную норму изменений, исключающих необходимость предоставлять в суд при обжаловании судебный акт, изготовленный в электронной форме.

Определяя важность электронного правосудия и важность роли, которую играет электронный документооборот, следует отметить, что он присущ самым разнообразным сферам общественных отношений, не ограничивается системой органов государственной власти, выступает инновационным средством в юридической деятельности. При этом, учитывая объем необходимого формального документооборота, в настоящее время не сформировался единый механизм идентификации подлинности документов. В частности, формируется механизм электронного документооборота, например, для дистанционного заключения гражданско-правовых договоров, обсуждается необходимость разработать эффективный алгоритм и статус электронной подписи участников

договорных отношений¹¹. Это, как представляется, демонстрирует, что рассматриваемая проблема не ограничивается деятельностью исключительно судебной ветви власти, а требует комплексного охвата проблематики различных сфер общественной жизни.

Таким образом, проведенное исследование позволяет сделать вывод, что понятия «электронное правосудие» и «электронный документооборот» соотносятся как общее и частное, хотя последний и составляет значительную часть электронного правосудия на практике. Электронный документооборот в судах может быть определен в качестве формы осуществления

процессуальных действий посредством информационных технологий. Ключевыми элементами электронного документооборота в судах в настоящее время являются возможность подачи искового заявления в электронной форме, возможность изготовления и обращения судебного акта в электронной форме и т. д. Соответственно, можно сделать вывод, что электронный документооборот в судах способствует сокращению временных и финансовых издержек. Тем не менее, направления для совершенствования электронного документооборота в судах общей юрисдикции еще имеются.

Список литературы

1. Борисова Л. В. Электронное правосудие как форма судебной защиты в России // Актуальные проблемы российского права. 2020. Т. 15, № 6 (115). С. 105–111.
2. Брянцева О. В. Электронное правосудие в России: проблемы и пути решения / О. В. Брянцева, О. Л. Солдаткина // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 12 (64). С. 97–104.
3. Валеев Д. Х. Электронный документооборот в сфере правосудия в условиях цифровой экономики / Д. Х. Валеев, А. Г. Нуриев // Вестник Пермского университета. Юридические науки. 2019. № 45. С. 467–489.
4. Воронцова И. В. О соотношении понятий «электронный суд» и «электронное правосудие» // Правовая политика и правовая жизнь. 2019. № 3. С. 167–169.
5. Гордиенко Е. Л. Электронное правосудие: генезис и перспективы // Научные горизонты. 2019. № 5-1 (21). С. 129–135.
6. Кузьмин А. В. Электронная путёвка как новый институт договорного права: перспективы эффективности / А. В. Кузьмин, Е. В. Ивина // Новеллы права и политики 2018: в 2 т.: сборник научных трудов по материалам международной

¹¹ Кузьмин А. В., Ивина Е. В. Электронная путёвка как новый институт договорного права: перспективы эффективности // Новеллы права и политики 2018: в 2 т.:

сборник научных трудов по материалам международной научно-практической конференции (г. Гатчина, 30 ноября 2018 г.). Гатчина: Изд-во. ГИЭФПТ, 2019. Т. 1. С. 118.

научно-практической конференции (г. Гатчина, 30 ноября 2018 г.). Гатчина: Изд-во. ГИЭФПТ, 2019. Т. 1. С. 115–119.

7. Семушин А. В. Электронное правосудие в России – этапы и механизмы реализации // Актуальные проблемы инновационного педагогического образования. 2019. № 1. С. 40–43.

8. Трофимов Я. В. Сущность понятия «электронное правосудие» в процессуально-правовой доктрине // Форум. Серия: Гуманитарные и экономические науки. 2020. № 3 (20). С. 34–39.

Ekaterina V. Beloshitskaya

Assistant Judge of the Petrogradsky District Court of Saint Petersburg
(Saint Petersburg, Russian Federation)
beloshickaya-eka@mail.ru

ELECTRONIC DOCUMENT FLOW IN COURTS OF GENERAL JURISDICTION

Abstract: The article describes the state of electronic justice in the Russian state, focusing on such an element as electronic document management in courts of general jurisdiction. An extensive regulatory framework is used, the main directions of electronic document management are analyzed, problems associated with it are identified and ways to solve them are proposed.

Keywords: electronic justice, civil procedure, administrative procedure, criminal procedure, electronic document, electronic document, judicial act.

УДК 35

Хасан Самер Хажар

Аспирант,

Санкт-Петербургский государственный университет

(г. Санкт-Петербург, Российская Федерация)

Samerhasan816@gmail.com

НОРМАТИВНАЯ ЗАКОНОДАТЕЛЬНАЯ БАЗА, РЕГЛАМЕНТИРУЮЩАЯ ОКАЗАНИЕ ГОСУДАРСТВЕННЫХ УСЛУГ

Аннотация: В статье проведен анализ нормативно-правовых актов, регламентирующих оказание государственных услуг, обработки и хранения сведений, необходимых для выполнения органами государственной власти основных функций через применение информационных технологий, основные направления оптимизации предоставления государственных услуг, ключевые понятия и направления развития.

Ключевые слова: административный регламент, орган, управление, государственная услуга, закон.

Для цитирования:

Хасан С. Х. Нормативная законодательная база, регламентирующая оказание государственных услуг // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 279–282.

Нормативная законодательная база, регламентирующая оказание государственных услуг, представляет собой совокупность законодательных, нормативно-правовых и методических актов.

Конституция Российской Федерации является основным законом нашей страны и защищает права и свободы граждан РФ. В ст. 24 п. 1. Конституции РФ четко обозначено, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются, это очень важно при предоставлении

государственных услуг. А ст. 29 п. 4 гласит, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом. В ст. 33 Конституции РФ говорится о том, что граждане РФ имеют право обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления¹.

¹ Конституция Российской Федерации (принята всенародным голосованием

12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ

В Кодексе РФ об административных правонарушениях прописана ответственность за нарушение порядка предоставления государственных услуг. Так, в ст. 5.39 рассматриваемого нормативного акта «Отказ в предоставлении информации» говорится о том, что: «Неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено федеральными законами, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации, за исключением случаев, предусмотренных законодательством, влечет наложение административного штрафа на должностных лиц в размере от одной тысячи до трех тысяч рублей»².

Ст. 5.59. называется «Нарушение порядка рассмотрения обращений граждан»: «Нарушение установленного законодательством Российской Федерации порядка рассмотрения обращений граждан должностными лицами государственных органов и органов местного самоуправления, влечет наложение административного штрафа в размере от пяти тысяч до десяти тысяч рублей»³.

Федеральный закон РФ «Об организации предоставления

государственных и муниципальных услуг» является первым законодательным актом в отечественной нормативно-правовой базе, регламентирующей оказание государственных услуг, который направлен, прежде всего, на обеспечение прав граждан при обращении в государственные и муниципальные органы. Федеральный закон определяет принципы и процедуру предоставления государственных (муниципальных) услуг, условия и порядок их оплаты, права заявителей и обязанности органов власти. В частности, граждане имеют право на полные, актуальные и достоверные сведения о государственных услугах, а также на их предоставление дистанционно в электронном виде; органы же, в свою очередь, должны оказывать их своевременно и согласно стандарту.

В данном федеральном законе заложены все основные направления оптимизации предоставления государственных услуг, ключевые понятия и направления развития. Например, в ст. 5 определены права заявителей при получении государственных и муниципальных услуг: при получении

от 30.12.2008 № 6-ФЗ, от 30.12.2008 № 7-ФЗ, от 05.02.2014 № 2-ФЗ, от 01.07.2020 № 11-ФЗ) // Собрание законодательства РФ. 2020. № 31. Ст. 4398.

² Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (с изм. и доп., вступ. в силу от 01.05.2019) // СПС «КонсультантПлюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 21.02.2021).

³ Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (с изм. и доп., вступ. в силу от 01.05.2019) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 21.02.2021).

государственных и муниципальных услуг заявители имеют право на⁴:

1. Получение государственной или муниципальной услуги своевременно и в соответствии со стандартом предоставления государственной или муниципальной услуги.

2. Получение полной, актуальной и достоверной информации о порядке предоставления государственных и муниципальных услуг, в том числе в электронной форме.

3. Получение государственных и муниципальных услуг в электронной форме, если это не запрещено законом, а также в иных формах, предусмотренных законодательством Российской Федерации, по выбору заявителя.

4. Досудебное (внесудебное) рассмотрение жалоб (претензий) в процессе получения государственных и муниципальных услуг.

5. Получение государственных и муниципальных услуг в многофункциональном центре в соответствии с соглашениями, заключенными между многофункциональным центром и органами, предоставляющими государственные услуги, и соглашениями, заключенными между

многофункциональным центром и органами, предоставляющими муниципальные услуги (далее – соглашения о взаимодействии), с момента вступления в силу соответствующего соглашения о взаимодействии.

Так как предоставление большинства услуг связано с получением информации, то следующим нормативным актом можно назвать Федеральный закон «Об информации, информационных технологиях и о защите информации»⁵. Закон регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации, за исключением отношений, возникающих при охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации⁶.

Федеральный закон приводит понятийный аппарат и механизмы регулирования в соответствии с практикой применения информационных технологий [ст. 3]. Определяет правовой статус различных категорий информации. Закрепляет положения о

⁴ Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (с изм. и доп., вступ. в силу с 01.04.2019) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_103023/ (дата обращения: 21.02.2021).

⁵ Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (с изм. и доп., вступ. в силу с 01.04.2019) // СПС

«КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_103023/ (дата обращения: 21.02.2021).

⁶ Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (с изм. и доп., вступ. в силу с 01.04.2019) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_103023/ (дата обращения: 21.02.2021).

регулировании создания и эксплуатации информационных систем [ст. 12]. Определяет общие требования к использованию информационно-телекоммуникационных сетей [ст. 15]. Устанавливает принципы регулирования общественных отношений, связанных с использованием информации.

Развитие государственных услуг является частью реформы

государственной службы и более комплексных преобразований в сфере управления в государственном секторе. Государственные услуги, направленные на удовлетворение потребностей в сфере государственного управления, вытекают из задач страны и функций, реализуемых соответствующими министерствами, ведомствами и службами.

Samer Kh. Hasan

Postgraduate student,
St. Petersburg State University
(Saint-Petersburg, Russian Federation)
Samerhasan816@gmail.com

REGULATORY LEGISLATIVE FRAMEWORK REGULATING THE PROVISION OF PUBLIC SERVICES

Abstract: The article analyzes the regulatory legal acts governing the provision of public services, processing and storage of information necessary for the performance of the main functions by public authorities through the use of information technology, the main directions for optimizing the provision of public services, key concepts and directions of development.

Keywords: administrative regulation, body, management, public service, law.

УДК 347.9

Буряков Кирилл Константинович

Магистрант,

Саратовская государственная юридическая академия

(г. Саратов, Российская Федерация)

Laustfast@yandex.ru

Научный руководитель – О. А. Бахарева, кандидат юридических наук, доцент
кафедры гражданского процесса

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ПРИНЦИПА ДИСПОЗИТИВНОСТИ ПРИ РАССМОТРЕНИИ ДЕЛ СУДАМИ ОБЩЕЙ ЮРИСДИКЦИИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация: Принцип диспозитивности – это основной отраслевой принцип гражданского процессуального права, занимающий ведущее место в системе принципов. В статье выявлены проблемы реализации принципа диспозитивности при рассмотрении дел судами общей юрисдикции с использованием информационных технологий.

Ключевые слова: гражданский процесс, диспозитивность, принцип диспозитивности, информация, информационные технологии.

Для цитирования:

Буряков К. К. Проблемы реализации принципа диспозитивности при рассмотрении дел судами общей юрисдикции с использованием информационных технологий // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 283–287.

Актуальность темы исследования определяется наличием проблем реализации принципа диспозитивности при рассмотрении дел судами общей юрисдикции с использованием информационных технологий.

В процессуальной науке принцип диспозитивности гражданского процесса является общепризнанным, так как именно этот принцип отвечает за ходом, развитием, изменением гражданских дел. Данный принцип отвечает за переход из одной стадии

гражданского процесса в другую, а также отвечает за прекращение гражданского процесса участвующим лицом в данном деле. Основная суть данного принципа заключается в определении основной цели и предмета иска, его применение, а также урегулирование объема требований. Тем самым суд всегда осуществляет независимую проверку законности выдвигаемых запросов и требований, учитывая права и свободу

каждого человека, участвующего в процессе¹.

Многие выводы по принципам гражданского права подвергаются спорным дискуссиям, но принцип диспозитивности не оспаривается в настоящее время. Потому что именно принцип диспозитивности должен соблюдаться на протяжении всего судебного процесса, то есть от принятия иска до выполнения решения суда.

Именно поэтому диспозитивность судебного процесса является весомой и значимой частью гражданского права. Из-за неоднозначности и большого охвата данного принципа числится большое разнообразие форм и теряется основная сущность диспозитивности.

Именно принцип диспозитивности определяет демократизм современного общества и является центром стыка разных идей и нормативно фиксирует интересы государства и человека.

Необходимо в соответствии с законом и нормами следить за тем, чтобы частное было выше публичного, так как именно это ведет к усилению диспозитивности и повышает личную ответственность и социальную активность граждан, давая больше возможностей для свободной инициативной

деятельности, в том числе по отстаиванию своих прав и свобод.

Если рассматривать принцип диспозитивности с правовой точки зрения, то можно сказать, что законного определения данный принцип не имеет, так как он исходит из отдельных частей Гражданского процессуального кодекса Российской Федерации.

В этих статьях говорится о том, что гражданин и участник гражданского процесса может пользоваться теми правами человека, которые представляет ему закон посредством законных документов.

Основные положения и сущность принципа диспозитивности заложены в Конституции Российской Федерации (ст. 46), где четко прописано то, что каждому гражданину гарантируется полная судебная защита его прав и свобод².

Как утверждает А. А. Демичев, принцип диспозитивности укрепляет нормативно-руководящие положения гражданского и арбитражного судопроизводства, которые являются началом процесса инициативных граждан, заинтересованных в каком-либо деле³.

Исследуя работы А. А. Демичева, можно выделить основные характеристики принципа диспозитивности:

¹ См.: Османов Ш. Г. Содержание принципа диспозитивности гражданского процесса // Проблемы совершенствования законодательства. Сборник научных статей студентов юридического факультета. Махачкала, 2019. С. 218.

² См.: Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования

01.07.2020) // Рос. газ. 1993. № 237; Официальный интернет-портал правовой информации <http://www.pravo.gov.ru>, публикация от 04.07.2020.

³ См.: Демичев А. А. Позитивистская классификация принципов гражданского процессуального права Российской Федерации // Арбитражный и гражданский процесс. 2015. № 7. С. 5.

- в процессуальных отношениях права и равенство определяются для соответствующих категорий субъекта;

- возможность точного осуществления прав и выбора граждан в судопроизводстве.

Если рассматривать гражданский процесс, то можно отметить, что начало процесса всегда определяется по заявлению заинтересованного гражданина, который непосредственно подает заявление в суд, чтобы защитить свои права и свободу.

Отметим, что из-за обширности диспозитивного принципа его возможности и границы действия размыты, поэтому необходимо изучить и сформулировать основную узаконенную информацию о спектре его действия.

Основная идея данного принципа была закреплена в новом кодексе, которая подтверждалась возможностью участника судопроизводства завершить или обжаловать решения суда в соответствии с законом. Потому Гражданский процессуальный кодекс Российской Федерации⁴ считается более демократичным в отношении этого принципа. Но все равно, как отдельный пункт кодекса он не укреплен и поэтому нуждается в нормативном закреплении в гражданском праве.

Нормативность является обязательным признаком правовых принципов, потому что принципы — это основные моменты, которые могут урегулировать гражданский процесс.

Исходя из того, что нормативность является обязательным для всех правовых принципов необходимо законодательно закрепить принцип диспозитивности, определить его содержание и особенности в гражданском процессе.

Сегодня широко развивается цифровое правосудие. Применение информационных технологий вызывает определенные правовые последствия в реализации принципа диспозитивности.

В основе построения системы электронной коммуникации должен лежать принцип диспозитивности, заключающийся в согласии сторон на такого рода процессуальные действия суда. Такое согласие обеспечит надежность взаимного обмена информацией, возможность идентификации заинтересованных лиц и проверки достоверности их волеизъявления. Реализация идеи диспозитивности в этом отношении обусловлена тем, что на данном этапе становления «электронного правосудия» в первоочередном порядке должны учитываться интересы участников процесса, а затем — уже и суда. Это имеет особое значение применительно к судам общей юрисдикции. Согласие на использование технологий «электронного правосудия» имеет отношение и к подаче документов в электронном виде, и к организации удаленного участия посредством

⁴ Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-

ФЗ // Собр. законодательства Рос. Федерации. 2002. № 46. Ст. 4532.

видеоконференцсвязи и к иным элементам⁵.

Однако иногда наблюдается и излишняя увлеченность заботой об интересах участников процесса. Так, к примеру, введение обязательного аудио-протоколирования не исключает составление протокола в письменной форме. Более того, активно внедряемое сейчас и дополнительное видео-протоколирование не предполагает исключение письменной формы протокола. Считаем, что от письменной формы в таких условиях следует отказаться. Может быть, ее стоит сохранить только для случаев, когда стороны об этом специально

ходатайствуют или при обжаловании судебного акта.

С другой стороны, имеются и такие элементы, которые могут и должны внедряться вне зависимости от воли лиц, участвующих в деле. Это обусловлено преимущественными интересами суда, государства, да и общества в целом. Такой подход должен рассматриваться как объективно обусловленное исключение из принципа диспозитивности. К ним можно отнести и организацию электронного документооборота, и фиксацию судебного заседания путем аудио-/видеозаписей, и размещение судебных актов в сети Интернет.

Список литературы

1. Демичев А. А. Позитивистская классификация принципов гражданского процессуального права Российской Федерации // Арбитражный и гражданский процесс. 2015. № 7. С. 5–10.
2. Османов Ш. Г. Содержание принципа диспозитивности гражданского процесса // Проблемы совершенствования законодательства. Сборник научных статей студентов юридического факультета. Махачкала, 2019. С. 218–220.
3. Праницкая Т. О. Информационные технологии в гражданском процессе / Т. О. Праницкая, И. В. Гурова // Актуальные проблемы деятельности подразделений УИС. Сборник материалов Всероссийской научно-практической конференции, в 2 т. Воронеж, 2020. С. 229–233.

Kirill K. Buryakov
Graduate student,
Saratov State Law Academy
(Saratov, Russian Federation)
Laustfast@yandex.ru

Scientific supervisor – O. A. Bakhareva, PhD (Law), Associate Professor of the
Department of Civil Procedure

⁵ Праницкая Т. О., Гурова И. В. Информационные технологии в гражданском процессе // Актуальные проблемы деятельности подразделений

УИС. Сборник материалов Всероссийской научно-практической конференции, в 2 т. Воронеж, 2020. С. 229.

PROBLEMS OF IMPLEMENTATION OF THE PRINCIPLE OF DISPOSITIVITY IN THE CONSIDERATION OF CASES BY COURTS OF GENERAL JURISDICTION USING INFORMATION TECHNOLOGIES

Abstract: The principle of dispositivity is the main branch principle of civil procedure law, which occupies a leading place in the system of principles. The article reveals the problems of implementing the principle of dispositivity in the consideration of cases by courts of general jurisdiction using information technologies.

Keywords: civil procedure, dispositivity, the principle of dispositivity, information, information technology.

Гриднев Владимир Сергеевич

Студент,

Саратовская государственная юридическая академия

(г. Саратов, Российская Федерация)

Vova.gridnev.2001@mail.ru

Рословец Кристина Сергеевна

Студент,

Саратовская государственная юридическая академия

(г. Саратов, Российская Федерация)

Roslovets.kr@mail.ru

Научный руководитель – Н. Б. Островская, кандидат юридических наук, старший преподаватель кафедры финансового, банковского и таможенного права

ПЕРСПЕКТИВЫ РАЗВИТИЯ НАЛОГОВОГО МОНИТОРИНГА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация: Статья представляется актуальной, поскольку она позволяет раскрыть тему информационного взаимодействия налогоплательщиков и налоговых органов с помощью налогового мониторинга. Статья внесет определенный вклад в дальнейшее исследование темы и поможет в разрешении проблем, связанных с налоговым мониторингом.

Ключевые слова: налоги, налоговый мониторинг, налоговая проверка, налоговый контроль, налогообложение, налоговые поступления, бюджет.

Для цитирования:

Гриднев В. С. Перспективы развития налогового мониторинга в условиях цифровизации / В. С. Гриднев, К. С. Рословец // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 288–291.

Актуальность рассматриваемой темы продиктована современными условиями формирования налогового законодательства. В обстоятельствах технологического прогресса происходит качественное изменение различных сфер жизнедеятельности человека, что требует совершенствования способов и методов контроля. Одним из таких «инструментов» стал налоговый

мониторинг, основополагающая функция которого выражается в контроле за своевременной уплатой налогов в бюджеты бюджетной системы РФ.

Термин «налоговый мониторинг» появился в налоговом законодательстве после успешного завершения пилотного проекта, проведенного в 2012–2013 году посредством информационного

взаимодействия крупнейших налогоплательщиков страны с налоговыми органами. Сокращение налоговых споров, снижение затрат на налоговое управление у налогоплательщиков, устранение налоговых правонарушений – положительные результаты применения налогового мониторинга.

Давая общую характеристику процедуры осуществления налогового мониторинга, следует отметить, что организациям, желающим участвовать в налоговом мониторинге, необходимо подать соответствующее заявление в налоговый орган по месту своего нахождения не позднее 1 июля года, предшествующего периоду, за который проводится налоговый мониторинг. Несмотря на небольшой временной промежуток существования рассматриваемого института, законодатель активно проводит улучшения последнего. В частности, подп. «г» п. 9 ст. 1 Федерального закона от 29 декабря 2020 г. № 470-ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации о налогах и сборах» вводит

автоматическое продление налогового мониторинга в случае, если заявления об отказе в проведении налогового мониторинга не было представлено организацией до 1 декабря года, являющегося предметом проверки¹. Подпунктом «б» п. 8 ст. 1 названного федерального закона предусмотрены иные основания для продления налогового мониторинга². Подпункт «б» п. 3 и п. 7 ст. 2 анализируемого нормативно-правового акта закрепляет право налогоплательщиков на возмещение НДС и акцизов в заявительном порядке³. Кроме того, согласно подп. «б» п. 4 ст. 2 ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации о налогах и сборах» указанные субъекты имеют право на освобождение от акцизов по некоторым операциям без представления банковской гарантии⁴.

Налоговый мониторинг имеет свои достоинства и недостатки. Среди преимуществ можно выделить следующие:

1) возможность избежать налогового контроля и спора по его результатам;

¹ О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации о налогах и сборах: федеральный закон от 29.12.2020 № 470-ФЗ // Собрание законодательства РФ. 2021. № 1. Ст. 7627.

² О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации о налогах и сборах: федеральный закон от 29.12.2020 № 470-ФЗ // Собрание законодательства РФ. 2021. № 1. Ст. 7627.

³ О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации о налогах и сборах: федеральный закон от 29.12.2020 № 470-ФЗ // Собрание законодательства РФ. 2021. № 1. Ст. 7627.

⁴ О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации о налогах и сборах: федеральный закон от 29.12.2020 № 470-ФЗ // Собрание законодательства РФ. 2021. № 1. Ст. 7627.

2) возможность создавать бизнес с учетом позиции налогового органа.

Сегодня закон позволяет организациям не только отреагировать на мотивированное мнение, но и действительно исправить выявленные ошибки. Если организация предполагает наличие налоговых рисков, она вправе запросить мотивированное мнение самостоятельно, а при необходимости предоставить собственные аргументы в ходе осуществляемой процедуры и составить план налогового учета исходя из позиции налоговиков.

Наряду с достоинствами налоговому мониторингу присущи недостатки.

Особое внимание уделяется открытию налогоплательщиками информации налоговым органам. Организации применяют всевозможные электронные системы учета, протоколы передачи данных и т. д.

Налоговый мониторинг не исключает контроль соответствия рыночных цен. Территориальные органы ФНС сообщают в центральный аппарат о фактах контролируемых сделок, а ФНС, соответственно, проводит по ним проверки. Мотивированное мнение по соответствию цен в таких сделках налоговыми органами не составляется.

Вышесказанное подтверждает спорный характер вопроса о переходе к налоговому мониторингу. Тем не менее, думается, что такой переход имеет место быть, поскольку:

Во-первых, налоговый мониторинг – это некий диалог ФНС и бизнеса. Компания открывает финансовую отчетность и отслеживает действия ФНС с помощью истории запросов, что в свою очередь показывает «прозрачность» данной системы.

Во-вторых, традиционные формы взаимодействия с надзорным органом устаревают, что дает возможность «новому поколению», а именно налоговому мониторингу, быть в числе лидеров.

В-третьих, внедрение цифровых систем налогового учета – это инвестиции в имидж современной компании, ведущей честный и открытый бизнес.

Таким образом, явным преимуществом налогового мониторинга перед другими видами налоговых проверок является открытое и оперативное решение спорных моментов в отчетной деятельности организаций, так как объем электронного обмена документами позволяет уполномоченным органам быстро запрашивать необходимую информацию и проверять налоговую отчетность.

Список литературы

1. Гатышина Е. И. Налоговый мониторинг как инновационный способ контроля / Е. И. Гатышина, Е. С. Лебедева, Е. О. Никитина // Наукоедение. 2017. № 5. С. 2–8

2. Клейменова М. О. Налоговое право: учебное пособие / под ред. Ю. Б. Рубин. М.: Проспект, 2008. 412 с.

3. Маркина М. В. Налоговое право: учебно-методическое пособие для практических занятий и самостоятельной работы. Ростов н/Д, 2017. 38 с.

4. Минвалиева М. С. Сущность налогового мониторинга // Экономика и общество в фокусе современных исследований: традиции и инновации: материалы III международной научно-практической конференции / отв. ред. Е. Г. Жулина. Саратов, 2015. С. 92–94.

Vladimir S. Gridnev

Student,

Saratov State Law Academy
(Saratov, Russian Federation)
Vova.gridnev.2001@mail.ru

Kristina S. Roslovets

Student,

Saratov State Law Academy
(Saratov, Russian Federation)
Roslovets.kr@mail.ru

Scientific supervisor – N. B. Ostrovskaya, PhD (Law), Senior Lecturer of the
Department of Financial, Banking and Customs Law

DEVELOPMENT OUTLOOK OF THE TAX MONITORING IN THE CONDITIONS OF DIGITALIZATION

Abstract: The article is relevant, because it allows us to reveal the topic of information interaction between taxpayers and tax authorities with the help of tax monitoring. The article will make a certain contribution to further research of the topic and will help in solving problems related to tax monitoring.

Keywords: taxes, tax monitoring, tax audit, tax control, taxation, tax revenues, budget.

Загребин Даниил Геннадьевич
Курсант, рядовой полиции
Санкт-Петербургский университет МВД России
(г. Санкт-Петербург, Российская Федерация)
danil_zagrebina@mail.ru

Научный руководитель – А. Ю. Пиддубринная, кандидат юридических наук,
доцент, доцент кафедры гражданского права и гражданского процесса

ЭЛЕКТРОННОЕ ПРАВОСУДИЕ В РОССИИ: ПРОБЛЕМНЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Аннотация: В статье представлена общая характеристика систем электронного правосудия, раскрываются проблемные аспекты их использования. Автором выдвигаются варианты решения по устранению недостатков и рассмотрения перспектив дальнейшего развития и расширения сферы применения систем электронного правосудия.

Ключевые слова: электронное правосудие, суд, судопроизводство, гражданский процесс, уголовный процесс.

Для цитирования:

Загребин Д. Г. Электронное правосудие в России: проблемные аспекты применения и перспективы развития // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 292–300.

Стремительное развитие информационных технологий, внедрение их во все сферы общественных отношений не могло не затронуть такую важную сферу деятельности государства, как судопроизводство. Использование достижений науки и техники, современных технологий и информационных систем стало принципом работы не только органов государственной власти¹, но и всей судебной системы.

В этой связи, интересно обратиться к опыту некоторых зарубежных стран, где так называемое «цифровое правосудие» стало активно внедряться, раньше, чем в Российской Федерации.

В целях оптимизации работы судебных органов в ряде зарубежных стран разработана и эффективно применяется система электронного правосудия под общим названием e-justice. Поскольку, четко и единообразного понятия электронного

¹ О полиции: федеральный закон от 7 февраля 2011 г. № 3-ФЗ // СПС «Консультант Плюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_110165/ (дата обращения: 07.03.2021).

правосудия не закреплено, мы будем понимать совокупность различных автоматизированных информационных систем-сервисов, предоставляющих средства для публикации судебных актов, ведения электронного дела и доступа сторон к материалам электронного дела². Основной задачей таких систем является обеспечение гласности, открытости и доступности судопроизводства, упрощение приема подачи документов путем загрузки их в единую базу, популяризация деятельности судебных органов, ведущая к увеличению правовой грамотности населения, возможность проверки состояния судебного иска в любое удобное время и проведение судебных заседаний в режиме онлайн с использованием информационно телекоммуникационной сети интернет.

Одни из первых систем электронного правосудия были разработаны в Соединённых Штатах Америки под названиями Public Access to Court Electronic Records (PACER) и Case Management / Electronic Case Files (CM/ECF). Их основной задачей является электронная подача документов в суды, доступ к судебным электронным записям, ознакомление с историей принятых решений, доступ к календарю судебных заседаний.

В Российской Федерации, в частности в судах общей юрисдикции,

применяется и используется система ГАС «Правосудие», которая обеспечивает административный порядок деятельности судов. Однако возможности ее применения для участников процесса сводятся к минимальным. Так, гражданам предоставляется информация о деятельности судебной системы через интернет-портал, частичный доступ к банку судебных решений, судебная статистика, возможность хранения и ввода документов, необходимых для судебного разбирательства – т. е. фактически ГАС «Правосудие» носит информационно-справочный характер.

В арбитражных судах на сегодняшний день, возможности электронного правосудия существенно шире. Так, система электронного правосудия «Мой Арбитр» позволяет подавать заверенные электронные образцы документов или непосредственно электронные документы, подписанные электронной подписью, использовать систему видео-конференц-связи для разрешения судебного дела. На 13 июля 2020 года к системе веб-конференции было подключено 90 арбитражных судов, проведено 19 213 онлайн-заседаний, при этом назначено к рассмотрению еще 30 131 заседаний, а всего подано 59 381 ходатайств о проведении судебных заседаний в онлайн-режиме. Таким образом, можно утверждать,

² Сидоров Ю. В. Отличия в понимании сущности электронного правосудия в России и за рубежом // Ученые записки Петрозаводского государственного университета. 2015. № 5 (150). С. 108–111. Режим доступа: Научная электронная

библиотека «КиберЛенинка». URL <https://cyberleninka.ru/article/n/otlichiya-v-ponimanii-suschnosti-elektronnogo-pravosudiya-v-rossii-i-za-rubezhom> (дата обращения: 07.03.2021).

что в арбитражной судебной системе успешно применены современные IT-технологии, которые помогли судам в полном объеме вершить правосудие онлайн, что позволяет нам сделать вывод об эффективности их применения.

Дополнительным катализатором в развитии электронного правосудия, послужило введение ограничений на очное судебное разбирательство, связанное с распространением новой коронавирусной инфекции COVID-19. В период с 18 марта по 20 апреля 2020 года в суды поступили 225,2 тыс. документов в электронном виде – на 77,3 тыс. документов больше, чем за аналогичный период предыдущего года (с 18 марта по 20 апреля 2019 года в суды было подано 147,9 тыс. документов в электронном виде)³, однако в период с 18 марта по 20 апреля 2020 года было проведено всего 8 тыс. судебных заседаний с использованием систем видео-конференц-связи.

На сегодняшний день, на базе сервиса «Госуслуги» разрабатывается система «Правосудие онлайн», являющаяся одной из самых перспективных систем в области применения электронного правосудия в мире. В 2020 году была введена автоматическая территориальная подсудность дел. В период с 2021 по 2024 года планируется реализовать возможность получать уведомления и документы в электронном виде, знакомиться с материалами дела в личном кабинете, получать консультации от «интерактивного

помощника», оплачивать госпошлины, рассчитанные автоматически на основании заявленных в иске требований, возможность удалённого участия в судебном процессе, введение биометрической аутентификации участника судебного процесса.

На наш взгляд считается обоснованным введение системы видео- и аудиопротоколирования с распознаванием речи и последующим автоматическим транскрибированием. Данное введение позволит участникам процесса максимально детально восстановить ход судебного заседания и уменьшит количество жалоб, связанных с протоколированием, подаваемых в суды апелляционной или кассационной инстанции. Также стоит уделить внимание созданию защищенных каналов связи, защите персональных данных, в целях недопущения срыва судебных заседаний путем применения DOS-атак, сниффинговых пакетов, искажения фактов путем внесения изменений в документы и распространения личной информации участников процесса. Для упрощения подачи документов необходимо привести бланки исковых требований к установленным законом образцу с возможностью интерактивного заполнения.

Однако при наличии существенных достоинств, система электронного правосудия не сможет стать полноценной альтернативой традиционной форме судопроизводства. За период действия

³ Работа отечественных судов в условиях пандемии // Верховный Суд Российской Федерации: официальный сайт. Дата

обновления: 21.04.2020. URL: http://www.supcourt.ru/press_center/news/28858/ (дата обращения: 07.03.2021).

карантинных мероприятий в период пандемии COVID-19 было подано свыше 200 тысяч судебных исков, при этом рассмотрено было только 22 тысячи, что составляет 11 % от общего количества заявлений. В этой связи 29 апреля 2020 г. Президиум Верховного Суда Российской Федерации и Президиум Совета судей Российской Федерации вынесли постановление № 822, в котором судам было рекомендовано дальнейшее рассмотрение дел путем использования видео-конференц-связи⁴.

Данный факт позволяет судить о частичной работоспособности сервисов электронного правосудия.

Пандемия COVID-19 сильно повлияла на общественную жизнь и работу государственных институтов, в том числе и судебной власти. Судьям и сотрудникам судов пришлось работать с риском для здоровья, при постоянно меняющихся обстоятельствах и дополнительной нагрузке из-за потока дел, связанных с нарушением новых правил. Суды разных уровней были вынуждены реагировать на чрезвычайную ситуацию: организовать работу в новых условиях, трактовать и применять нормативные акты, принятые из-за распространения вируса, а также следить за законностью и пропорциональностью карантинных мер.

В чрезвычайных условиях проявились недостатки законов: спорные места и пробелы в

регулировании, которые активно пытался исправить Верховный суд.

Именно Верховный суд, замещая законодателя, в середине марта ограничил работу нижестоящих судов, чтобы избежать распространения вируса. Согласно Конституции, такие меры ограничивали фундаментальное право граждан на справедливое судебное разбирательство. Ограничения, которые вводил и снимал Верховный суд, не всегда соотносились с действиями исполнительных властей – главного государственного санитарного врача, глав регионов. Иногда сочетание действий Верховного суда и исполнительных властей только усугубляло ущемление прав.

Пандемия показала, насколько ценна возможность проводить онлайн-заседания. В марте Совет Федерации запустил обсуждение о легитимизации онлайн-заседаний, но за полгода инициативу не реализовали. Тем временем Верховный суд в апреле разрешил судам использовать для проведения заседаний не только видео-конференц-связь, но и веб-конференции, предполагающие подключение с личных устройств.

Как показала практика, районные суды оказались не готовы к дистанционному рассмотрению дел. Еще с конца марта некоторые заседания начинают проводиться с использованием мессенджеров, таких как WhatsApp или Skype, в которых невозможно идентифицировать

⁴ Постановление Президиума Верховного Суда РФ и Президиума Совета судей РФ от 29 апреля 2020 г. № 822 // СПС

«Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_351604/ (дата обращения: 07.03.2021).

участников процесса и гарантировать безопасность передачи данных.

Суд в Кемерово во время заседания по WhatsApp отклонил ходатайство об участии защитника, находящегося в Москве. Истец выступил против, сославшись на то, что, если адвокат прилетит из Москвы, он «будет помещен в изоляцию», а при веб-конференции невозможно будет «удостоверить его полномочия». Связь на заседании была настолько плохая, что ответчик не понял, что в ходатайстве было отказано и в суде участвовал адвокат по назначению.

При рассмотрении в Мосгорсуде дела Константина Котова 16 апреля защитники ходатайствовали о допросе свидетеля по видеосвязи⁵. По словам адвоката, судья отказал в ходатайстве, сославшись на то, что Постановление Верховного суда не является законом.

Также открытыми остается ряд вопросов, таких как предоставление оригиналов документов, поданных в электронном виде (ст. 71 ГПК РФ). В настоящее время все чаще документы сразу создаются в электронной форме (например, платежное поручение, подготовленное с использованием системы «банк-клиент»), и тогда возникает вопрос о том, что считать оригиналом, а что – копией документа. Вероятно, данная норма потребует дальнейшего уточнения.

Арбитражный суд оценивает письменные доказательства, иные документы и материалы, представленные путем использования систем видео-конференц-связи, в

совокупности и взаимосвязи с другими доказательствами по делу (ст. 71 АПК РФ). Копии таких документов незамедлительно направляются в суд, рассматривающий дело, по факсимильной связи или электронной почте либо с использованием иных средств связи. При этом вещественные доказательства не могут быть представлены для осмотра посредством использования систем видео-конференц-связи и представляются в суд для их исследования в судебном заседании согласно требованиям, ст. 162 АПК РФ. Таким образом, данный пробел в законодательстве не позволяет судам объективно рассмотреть дело и в полной мере оценить доказательную базу участников судебного разбирательства.

Документы, поданные в электронной форме, во всех установленных случаях, являются лишь отсканированным видом бумажного документа. Невозможность интерактивно заполнить документ обязывает участника процесса фактически создать документ на материальном носителе. Электронная форма документа выполняет лишь «транспортную» функцию, необходимую лишь в период, предшествующий самому судебному разбирательству.

К тому же достаточно трудно подавать в суды материалы посредством электронных форм большого объема, поскольку

⁵ Информация по делу № 10-5350/2020 // Официальный портал судов общей юрисдикции города Москвы URL:

<https://mos-gorsud.ru/mgs/services/cases/appeal-criminal/details/bc40e9ea-13aa-4380-91dc-6542bc4ddbb6> (дата обращения: 10.03.2021).

возникает необходимость перевода документов в формат Adobe PDF. Отметим, что при выборе необходимой опции в подсистеме «Мой арбитр» не всегда можно найти свой документ, то есть тот документ, который подлежит подаче в конкретном деле на конкретном этапе разбирательства (например, «Письменные объяснения в порядке ст. 81 АПК РФ»).

В случае возникновения технических неполадок, как указывалось выше, согласно ст. 158 АПК РФ, такая проблема может стать легальным основанием для отложения судебного разбирательства, что никак не приводит к ускорению процесса.

Отдельного внимания заслуживает упрощенный порядок рассмотрения дел (глава 29 АПК РФ). Здесь в усиленном режиме реализуется электронное правосудие, поскольку такой порядок позволяет участникам процесса в режиме удаленного доступа не только пользоваться судебными актами, но и просматривать все процессуальные документы, содержащиеся в материалах дела и исходящие от сторон. Однако такой порядок исключает возможность участия в «электронном деле», рассматриваемом в порядке главы 29 АПК, третьего или иного заинтересованного лица (с его вступлением в процесс осуществится переход на общие правила искового производства). Таким образом,

переход на общие правила иска обнуляет все достижения электронного правосудия, характеризующие порядок упрощенного производства.

Также отметим, что в настоящее время в АПК РФ имеются нереализуемые элементы электронного правосудия. К числу таких отнесем процедуру выдачи исполнительного листа, когда исполнительный лист может направляться судом для исполнения в форме электронного документа, подписанного судьей, усиленной квалифицированной электронной подписью (ч. 3 ст. 319 АПК РФ).

Стоит упомянуть, что нормами процессуального законодательства не предусмотрена возможность обжалования определений об отказе в удовлетворении ходатайства об участии в судебном заседании путем использования видео-конференц-связи⁶.

Также остро стоит вопрос десакрализации всей судебной системы. Судьи, будучи консервативной частью сообщества, смотрят на процесс цифровизации судов с настороженностью. Любые новшества могут повлечь нарушения прав в процессе. Тем не менее в целом они понимают важность электронного правосудия и готовы идти в ногу со временем. Остаются вопросы, связанные с «десакрализацией» правосудия. Судебное сообщество обсуждает, как вести себя во время

⁶ Постановление Арбитражного Суда Центрального Округа от 13.08.2015 по делу № А64-2117/2015 // Карточка арбитражных дел. URL: [https://kad.arbitr.ru/Document/Pdf/c662d094-8914-4b0e-a01a-](https://kad.arbitr.ru/Document/Pdf/c662d094-8914-4b0e-a01a-0a4824da3f39/a66bb4e9-9d95-4248-aa2e-0758169602b1/A64-2117-015_20150813_Reshenija_i_postanovlenija.pdf?isAddStamp=True)

[0a4824da3f39/a66bb4e9-9d95-4248-aa2e-0758169602b1/A64-2117-015_20150813_Reshenija_i_postanovlenija.pdf?isAddStamp=True](https://kad.arbitr.ru/Document/Pdf/c662d094-8914-4b0e-a01a-0a4824da3f39/a66bb4e9-9d95-4248-aa2e-0758169602b1/A64-2117-015_20150813_Reshenija_i_postanovlenija.pdf?isAddStamp=True) (дата обращения: 09.03.2021).

дистанционного процесса: можно ли обойтись без флага, герба или мантии и надо ли вставать при оглашении судебного решения.

Другой вопрос – открытость процесса, один из основных его принципов. Пока не совсем ясно, как именно обеспечить доступ к онлайн-заседанию. Открытые трансляции на видеохостингах – это слишком, считают юристы, но и разрешительный порядок участия в открытом заседании – это не лучшая идея. В целях обеспечения гласности и открытости процесса на наш взгляд считается разумным создание онлайн-комнат судебных заседаний с персональной авторизацией для граждан, интересующихся определенным процессом. При этом стоит учесть доступное количество мест для обеспечения работоспособности серверов.

Важно сочетать девиртуализацию правосудия с необходимостью соблюдения основных процессуальных прав, резюмировал Владимир Владимирович Ярков, завкафедрой гражданского процесса УрГЮУ, профессор ИЦЧП им. Алексеева. В сегодняшней ситуации он отдельно отметил, что Верховный суд воспользовался возможностью применить аналогию права и использовал потенциал кодексов, чтобы найти новые формы общения для участников процессов и не изменять законодательство.

Владимир Владимирович Ярков также задается вопросом о строгой подсудности дел, так как с появлением онлайн-правосудия появляется

возможность равномерно распределить нагрузку между судами.

Говоря об онлайн-правосудии, необходимо понимать, что возможность провести заседание онлайн в обычное время для сторон должно оставаться удобной опцией, но вовсе не обязанностью. Одна из причин – онлайн-процесс подходит в равной степени не для всех видов судопроизводства. Арбитражное судопроизводство, которое пришло из письменной процедуры, сегодня наиболее близко к цифровой трансформации.

При этом уголовное судопроизводство должно наименьшим образом участвовать в цифровизации, в связи со спецификой общественных отношений, охраняемых уголовным законом. Одной из ключевых причин можно назвать злоупотребления из-за необъяснимого прерывания связи: «Когда это выгодно кому-то из сторон». При этом суду сложно оперативно понять, из-за чего произошел сбой. Еще одним из проблемных аспектов можно выделить объявление перерыва в судебном заседании (ст. 253 УПК РФ) для общения защитника с подсудимым – если защитник и подсудимый используют при диалоге систему ВКС ничто не может гарантировать конфиденциальность их разговора.

Более существенной проблемой представляется рассмотрение дел в закрытом порядке судебного разбирательства, регламентированных ст. 241 УПК РФ. Возможность использования видео-конференц-связи не может быть осуществлена,

так как данный порядок судопроизводства не обеспечивает должным образом информационную защиту материалов уголовного дела, интересов граждан и государства.

Так же малоперспективным направлением можно выделить рассмотрение уголовного дела с участием суда присяжных. Возникает ряд вопросов, таких как подача вопросов председательствующему после допроса подсудимого, потерпевшего, свидетелей, эксперта (ст. 335 УПК РФ), обеспечение тайны совещания присяжных заседателей (ст. 341 УПК РФ), возникновение технических неполадок во время заседания, возможность повлиять на решение присяжных извне.

Подводя итог о проблемных особенностях дистанционного правосудия, стоит отметить, что

онлайн-правосудие – это не универсальный выход для замены очных процессов. Несмотря на пройденные стадии внедрения, остаётся достаточно обширная область для цифровизации и создания узкопрофильных систем электронного правосудия, каждая из которых в свою очередь будет требовать детальной проработки и вновь прохождения этапа становления. Но будет упущением не отметить, что в связи с тяжелой эпидемиологической ситуацией, которая в свою очередь послужила неким катализатором к массовому применению электронного правосудия, данный вид систем показал себя с той технологичной стороны, которая и демонстрирует нам насколько это необходимо и широко применимо для нас как сейчас, так и в ближайшем будущем.

Список литературы

1. Алешкова И. А. Судебная власть в условиях новой информационной реальности / И. А. Алешкова, О. Х. Молокаева // Государство и право в новой информационной реальности. 2018. № 1. С. 82–98. Режим доступа: Научная электронная библиотека «КиберЛенинка». URL: <https://cyberleninka.ru/article/n/sudebnaya-vlast-v-usloviyah-novoy-informatsionnoy-realnosti>.
2. Денисов И. С. Развитие электронного правосудия в России // Вестник Санкт-Петербургского университета МВД России. 2018. № 1 (77). С. 101–104. Режим доступа: Научная электронная библиотека «КиберЛенинка». URL: <https://cyberleninka.ru/article/n/razvitie-elektronnogo-pravosudiya-v-rossii>.
3. Иванова С. А. Проблемы развития системы электронного правосудия / С. А. Иванова, В. А. Мирошникова // Образование и право. 2020. № 4. С. 234–239. Режим доступа: Научная электронная библиотека «КиберЛенинка». URL: <https://cyberleninka.ru/article/n/problemy-razvitiya-sistemy-elektronnogo-pravosudiya>.
4. Мухина А. В. К вопросу о понятии электронного правосудия / А. В. Мухина, М. А. Мокосеева // StudNet. 2020. № 12. С. 1566–1572. Режим доступа: Научная электронная библиотека «КиберЛенинка». URL: <https://cyberleninka.ru/article/n/k-voprosu-o-ponyatii-elektronnogo-pravosudiya>.

5. Работа отечественных судов в условиях пандемии // Верховный Суд Российской Федерации: официальный сайт. Дата обновления: 21.04.2020. URL: http://www.supcourt.ru/press_center/news/28858/.

6. Сидоров Ю. В. Отличия в понимании сущности электронного правосудия в России и за рубежом // Ученые записки Петрозаводского государственного университета. 2015. № 5 (150). С. 108–111. Режим доступа: Научная электронная библиотека «КиберЛенинка». URL: <https://cyberleninka.ru/article/n/otlichiya-v-ponimanii-suschnosti-elektronnogo-pravosudiya-v-rossii-i-za-rubezhom>.

7. Цифровизация судебной системы: анализ социальных сетей Верховного суда РФ // РАПСИ: Российское агентство правовой и судебной информации. URL: http://rapsinews.ru/judicial_analyst/20201211/306583524.html.

Daniil G. Zagrebina

Cadet,

St. Petersburg University of the Ministry of Internal
Affairs of Russia

(St. Petersburg, Russian Federation)

danil_zagrebina@mail.ru

Scientific supervisor – A. Yu. Piddubrivnaya, PhD (Law),
Associate Professor, Associate Professor of the
Department of Civil Law and Civil Procedure

E-JUSTICE IN RUSSIA: PROBLEMATIC ASPECTS OF APPLICATION AND DEVELOPMENT PROSPECTS

Abstract: The article presents a general characteristic of e-justice systems, reveals the problematic aspects of their use. The author puts forward options for solving the shortcomings and considering the prospects for further development and expansion of the scope of application of e-justice systems.

Keywords: e-justice, court, legal proceedings, civil procedure, criminal procedure.

УДК 347

Зверева Екатерина Дмитриевна

Студент,

Санкт-Петербургский юридический институт (филиал)

Университета прокуратуры Российской Федерации

(г. Санкт-Петербург, Российская Федерация)

Zvereva.E.D@yandex.ru

Научный руководитель – М. Ю. Порохов, кандидат юридических наук

ЦИФРОВИЗАЦИЯ СИСТЕМЫ ИСПОЛНИТЕЛЬНОГО ПРОИЗВОДСТВА В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: В статье рассматриваются этапы цифровизации системы исполнительного производства в Российской Федерации. Автором приведены и проанализированы преимущества и риски электронного документооборота между гражданами, организациями и судебными приставами-исполнителями, а также выявлена проблема извещения лиц, участвующих в исполнительном производстве, через «суперсервис». В заключении указаны перспективы использования информационных технологий, сделаны соответствующие выводы.

Ключевые слова: цифровая экономика, цифровизация, исполнительное производство, суперсервис, электронный документооборот.

Для цитирования:

Зверева Е. Д. Цифровизация системы исполнительного производства в Российской Федерации // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 301–306.

Современные технологии стремительно продвигаются вперёд и устанавливают перед обществом задачи по автоматизации управленческих процессов и развитию электронного правительства. Наблюдается общемировая тенденция к совершенствованию методов исполнительного производства, где российская модель наравне с зарубежными моделями

принудительного исполнения судебных актов постепенно переходит в электронно-цифровую среду¹.

Так, с 2012 года в России функционирует Банк данных исполнительных производств, ведение которого в электронном виде осуществляется средствами государственной информационной системы «Автоматизированная информационная система

¹ Шепелёва О. А. Перспективы развития исполнительного производства // Молодой учёный. 2020. № 51 (341). С. 318.

Федеральной службы судебных приставов», а с 2015 года был введён в эксплуатацию модуль ГАС «Правосудие», который обеспечивает взаимодействие национальной судебной системы и ФССП России в части передачи исполнительных документов в соответствии с форматами, принятыми Постановлением Правительства от 20 октября 2015 г. № 1121 «Об утверждении требований к форматам исполнительных документов, вынесенных и (или) направляемых для исполнения в формате электронного документа», через который возможно направить исполнительный документ в форме электронного документа, подписанного судьёй усиленной квалифицированной электронной подписью.

Поскольку дальнейшее расширение и оптимизация использования службой судебных приставов информационных технологий является залогом эффективного построения системы исполнительного производства, а также повышения открытости и доступности, большое внимание уделяется Цифровому государственному управлению. Это один из шести федеральных проектов национальной программы «Цифровая экономика», направленный на окончательный переход на электронное взаимодействие граждан с государством.

В настоящее время продолжается процесс внедрения «суперсервиса» – «Цифровое исполнительное производство». Площадкой взаимодействия выступает Единый портал

государственных и муниципальных услуг. Этот проект рассчитан на 3 года и планируется к завершению до конца 2021 года.

«Суперсервис» в результате полной реализации позволит представителям бизнеса и гражданам, которые являются сторонами исполнительного производства, взаимодействовать с ФССП РФ по различным вопросам удалённо, а необходимая информация будет предоставляться в автоматическом режиме онлайн. Помимо этого, с помощью сервиса Госуслуг будет доступно погашение задолженности до возбуждения исполнительного производства.

Условно цифровизацию исполнительных систем и внедрение «суперсервиса» можно разделить на несколько этапов.

Во-первых, с 26 ноября 2020 года все граждане могут подавать ходатайства, обращения, отводы и жалобы в рамках исполнительных производств через единый портал Госуслуг, с 27 октября 2020 года они могут получать информацию о ходе исполнительного производства, в том числе в виде расширенных выписок, при условии, что они зарегистрированы в качестве пользователей, а также сделали отметку, что готовы получать данные документы, как юридически значимые.

К маю 2021 года данный этап считается исполненным, несмотря на то что полностью не учтены права индивидуальных предпринимателей и юридических лиц. Вероятно, здесь проявляется проблема подтверждения полномочий их представителей.

Второй этап в виде осуществления исполнительного производства через реестровую модель не исполнен до конца, поскольку практически полностью зависит от органов, уполномоченных к вынесению исполнительных документов. Здесь наблюдается прямая зависимость между техническим оснащением данных органов, большим объёмом исполнительных документов в письменной форме и порядком участия в работе данного сервиса. Как только контрагенты, с которыми до сих пор не налажен контакт, будут готовы к направлению исполнительных документов в электронном формате и исполнению положений, которые предусматривает «Цифровое исполнительное производство», можно будет говорить о завершении этапа.

Исходя из сказанного, к 2022 году планируется переход на реестровую модель принудительного исполнения, что исключит из оборота исполнительные документы в бумажном виде.

За последние годы Федеральная служба судебных приставов РФ не смогла продвинуться в цифровизации своих услуг. Между тем, в ведомство увеличивается поток исполнительных производств по взысканию долгов с граждан и компаний, и ежегодный прирост дел составляет в среднем пятнадцать процентов. Цифровизация процедур исполнительного производства, как считается, способна автоматизировать и разгрузить приставов-исполнителей хотя бы частично.

Среди проблем цифровизации в Российской Федерации выделяется объективное переключение административных и экономических ресурсов в 2020 году в более нуждающуюся сферу общества, отсутствие достаточной нормативной базы, несвоевременное финансирование, низкая исполнительная дисциплина. Кроме этого, не стоит забывать, что ФССП РФ является судебным исполнителем и потому сильно зависит от степени цифровизации судебной системы.

Если выделять плюсы цифровизации, то прежде всего это оптимизация взаимодействия всех участников исполнительного производства, повышение их осведомлённости, обеспечение прозрачности работы судебных приставов, упрощение процесса исполнительного производства, сокращение количества личных контактов сторон исполнительного производства с сотрудниками ФССП РФ. Для сферы государственного управления – это повышение эффективности принудительного исполнения, сокращение нагрузки на работников службы, исполнение требований законодательства по уведомлению сторон исполнительного производства, повышение уровня удовлетворённости граждан качеством государственных сервисов.

Важнейшим достижением всех планируемых работ по цифровой трансформации исполнительного производства является значительное сокращение сроков различных исполнительных процедур. Так, сроки снятия ограничений на имущество при

этом по плану сократятся со 120 часов после оплаты долга до 40 минут, сроки рассмотрения ходатайств – с 240 часов до 35 минут.

«Суперсервис» позволит также упростить идентификацию пользователей, открывающих личный кабинет на ресурсах государственных органов, чтобы исключить возможность появления «двойников».

Однако, по утверждению К. Л. Брановицкого, активное использование современных технологий не обязательно приведёт к повышению доступности, поскольку для этого необходимо наличие устойчивой системы идентификации пользователей информационных систем, повышение квалификации сотрудников и соблюдение баланса между электронным и бумажным оборотом². Кроме того, нет гарантии существенного сокращения выделяемых денежных средств из бюджета при использовании электронного документооборота, поскольку уже осуществлены расходы на дорогостоящие системы информационной безопасности, системы идентификации, хранения данных и так далее.

С другой стороны имеются риски, характерные для процесса цифровизации в любой сфере деятельности – кибербезопасность, достоверность сведений в электронной форме, аутентичность данных и сведений в материалах дела. А если произойдёт техническое

отключение сетей или, как было в период карантина, прекращение работы сервиса, то принцип своевременности совершения исполнительных действий и применения мер принудительного исполнения и другие принципы обеспечить будет сложно.

В случае полного перехода на доступные функции «суперсервиса» наблюдается неразрешённый вопрос о извещении лиц, участвующих в исполнительном производстве. Согласно статье 24 Федерального закона от 2 октября 2007 года № 229-ФЗ «Об исполнительном производстве», судебные приставы-исполнители могут через личный кабинет физического лица на портале «Госуслуги» направлять извещения должникам о возбуждении исполнительного производства, времени и месте совершения исполнительных действий или применении мер принудительного исполнения.

Моментом доставки извещения при этом будет время, когда лицо, участвующее в исполнительном производстве, входило в личный кабинет с использованием единой системы идентификации и аутентификации. Далее уведомление о факте доставки передаётся в Федеральную службу судебных приставов РФ для принятия решения по исполнительному производству³.

² Брановицкий К. Л. Некоторые аспекты использования информационных технологий в исполнительном производстве // Вестник гражданского процесса. 2018. № 1. С. 88.

³ Грицай О. В. Цифровизация как способ оптимизации механизма защиты гражданских прав в сфере гражданской юрисдикции // Юридический вестник Самарского университета. 2019. № 2. С. 66.

Возникает проблема: как быть в случаях, если лицо на протяжении длительного промежутка времени намеренно не авторизовалось в личном кабинете, или в силу технической ошибки не могло воспользоваться сайтом «Госуслуг», или фактически не прочитало извещение, поскольку не заметило его в строке уведомлений. Можно ли считать такое лицо должным образом извещённым?

Законодатель предполагает, что судебный пристав-исполнитель сам определяет форму извещения, поэтому не обязан её согласовывать или подстраховаться, направляя его в письменной форме.

Цифровизация, несмотря на различного рода сложности, в разное время с нестабильной скоростью продолжается, что позволяет выявить перспективные направления развития информационных технологий в исполнительном производстве. Это не только разработка и ведение электронного реестра исполнительных документов в целях исключения двойного списания задолженностей и ранжирование электронных обращений на категории, но и расширение электронного

межведомственного взаимодействия ФССП РФ с судебной системой, органами государственной власти, банковской системой, в том числе в части создания и ведения Банка данных взаимосвязанных документов, обеспечивающего приставам-исполнителям непрерывный доступ и обработку массивов документов и обеспечение конфиденциальности данных при использовании сервиса «Судебная задолженность» на портале «Госуслуги»⁴.

На данный момент «суперсервис» не позволяет соотносить активы должника с его обязательствами для комплексной оценки исполнения его обязательств, однако такое развитие цифровизации могло бы стать актуальным.

Таким образом, цифровизация исполнительного производства в Российской Федерации имеет ключевое значение. Наравне с позитивными изменениями выделяются проблемные вопросы, к решению которых с целью избежать нарушение прав лиц, участвующих в исполнительном производстве, следует подходить весьма осторожно и внимательно.

Список литературы

1. Брановицкий К. Л. Некоторые аспекты использования информационных технологий в исполнительном производстве // Вестник гражданского процесса. 2018. № 1. С. 87–101.
2. Грицай О. В. Цифровизация как способ оптимизации механизма защиты гражданских прав в сфере гражданской юрисдикции / О. В. Грицай, Е. Н. Губина // Юридический вестник Самарского университета. 2019. № 2. С. 64–68.

⁴ Цирина М. А. Цифровизация исполнительного производства //

Международное публичное и частное право. 2020. № 1. С. 44–45.

3. Цирина М. А. Цифровизация исполнительного производства // Международное публичное и частное право. 2020. № 1. С. 42–45.

4. Шепелёва О. А. Перспективы развития исполнительного производства // Молодой учёный. 2020. № 51 (341). С. 318–319.

Ekaterina D. Zvereva

Student,

St. Petersburg Law Institute (branch) of the
University of prosecutor's office of the Russian Federation
(Saint Petersburg, Russian Federation)
Zvereva.E.D@yandex.ru

Scientific supervisor – M. Yu. Porokhov, PhD (Law)

DIGITALIZATION OF THE SYSTEM OF ENFORCEMENT PROCEEDINGS IN THE RUSSIAN FEDERATION

Abstract: The article deals with the stages of digitalization of the system of enforcement proceedings in the Russian Federation. The author presents and analyzes the advantages and risks of electronic document management between citizens, organizations and bailiffs, and also identifies the problem of notifying persons involved in enforcement proceedings through «superservice». In conclusion, the prospects for the use of information technologies are indicated, and the corresponding conclusions are made.

Keywords: digital economy, digitalization, executive production, superservice, electronic document management.

УДК 349

Круть Леонид Сергеевич

Студент,

Уральский Государственный Юридический Университет

(Екатеринбург, Российская Федерация)

leonidkrut3002@gmail.com

Научный руководитель – Е. В. Дженакова, старший преподаватель кафедры
информационного права

LEGAL TECH: ДРУГ ИЛИ ВРАГ ЮРИСТА?

Аннотация: С развитием технологий и постоянным изменением общественной жизни коррективы вносятся и в нашу с вами профессиональную сферу. Появляются новые технологии, которые своими возможностями и новшествами, на первый взгляд, стремятся обесценить профессию юриста. Функции новых роботов, целью которых является предоставление юридической помощи и консультация населения посредством прямого анализа норм права и юридической практики, не просто совпадают с функциями нашей профессии, но и существенно дополняют их, ориентируя нас при решении правовых задач с помощью формальных норм, определенных законодательством той или иной страны.

Вследствие этого возникает вопрос о популярности и востребованности данных IT-технологий на рынке юридических услуг, а также о перспективе исчезновения профессии юриста в будущем. Внедрение в повседневную рутинную работу специализированных машин, инструментов усиливает конкуренцию внутри нашей профессии и создает дополнительные условия, требования, не следуя которым, молодые юристы просто не смогут раскрыть свою профпригодность. Данный вопрос стоит ребром в обсуждениях у видных юристов нашего времени. Так, в 2018 году прошел самый настоящий поединок Р.С. Бевзенко с роботом, разработанным на основе нейронных сетей с использованием массивов данных, включающих судебную практику, деловую переписку, научные работы и правовые позиции юристов. Победу в нашумевших прениях одержал известный практикующий юрист, однако споры о возможностях роботов в юриспруденции не утихают до сих пор¹.

Ключевые слова: Legal tech, информатизация в юриспруденции, электронный судья, компьютерные технологии в юриспруденции, автоматизация юридической деятельности.

¹ Михайлова А. Юридический баттл: робот от МегаФон vs Роман // Право.Ру. 2018. 17 мая. URL: <https://pravo.ru/lf/story/202675/> (дата обращения: 15.05.2021).

Для цитирования:

Круть Л. С. Legal Tech: друг или враг юриста? // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 307–313.

Legal Tech (сокращ. от англ. legal technology) – это разнообразные платформы, программы, продукты и инструменты, специально разработанные для упрощения и оптимизации процессов, составляющих профессиональную деятельность юристов. Legal Tech представляет собой технологические решения, создаваемые для профессиональных юристов и юридического бизнеса с целью повышения эффективности оказания юридических услуг или юридического сопровождения бизнеса¹.

Предоставление потребителям юридических услуг с использованием информационных технологий реализуется посредством онлайн-посредничества между заказчиком и юридической фирмой либо предоставлением инструментов для юридического самообслуживания, исключающих необходимость обращения к профессиональным юристам.

В настоящее время Legal Tech включает в себя: справочно-правовые системы, конструкторы шаблонов документов, согласование документов и работы над их проектами

Развитие сегмента Legal Tech приводит к изменению целей, приоритетов и необходимых навыков

юристов, а также продуктов, которые упрощают труд специалистов. При этом одной из основных целей индустрии Legal Tech является переход к качественно новой системе правосудия, которая должна стать более доступной для миллионов людей во всем мире за счет использования различных инструментов автоматизации².

Основными предназначениями Legal Tech являются:

1. Повышение правовой грамотности населения:

Legal Tech предлагает инструменты, позволяющие производить юридическую оценку обстоятельств дела неспециалистами. Такие инструменты могут удовлетворить потребности малого бизнеса, позволяя существенно снизить расходы на содержание юридического отдела.

Новые технологии позволяют без помощи юристов анализировать и готовить правовые документы, частично автоматизируют процесс принятия решений по юридическим вопросам, а также помогают составлять черновики договоров, завещаний и прочих документов. В перспективе такой подход сможет уменьшить число ошибок,

¹ Рожкова М. А. LegalTech и LawTech – что это такое и в чем их значимость для права? // Закон.ру. 2020. 14 фев. URL: https://zakon.ru/blog/2020/02/14/legaltech_i_lawtech_-_%C2%A0что_ето_такое_i_v_chem_ih_znachimost_dlya_prava (дата обращения: 15.05.2021).

² Кузнецов А. Словарь юриста: Legaltech, Lawtech и Regtech // RUSBASE. 2019. 12 мар. URL: <https://rb.ru/story/law-dictionary/> (дата обращения: 15.05.2021).

сопровождающих юридические операции, за счет обработки всего массива правовых норм и судебной практики по отдельным категориям дел, а также сможет повысить доступность юридических услуг за счет снижения их стоимости, что может существенно снизить спрос на деятельность юристов.

2. Повышение эффективности работы юристов:

Инструменты, повышающие скорость подготовки и оценки правовых требований, могут упростить работу профессиональных юристов и позволяют специалистам концентрироваться на действительно важных задачах, не отвлекаясь на рутинную работу.

Например, одними из самых утомительных аспектов в юридической сфере являются исследование и поиск информации. Юристу необходимо слушать истории клиентов, проводить брифинги, собирать данные по контрагентам, изучать показания, чтобы найти факты, которые помогут выиграть дело. Порой объемы информации настолько велики, что на поиск может уйти много времени. Legal Tech же позволяет быстро найти наиболее важную информацию.

Использование справочных и информационных систем уменьшает издержки, связанные с правовым анализом дела, а также позволяет более точно оценить перспективы судебного разбирательства, основываясь на результатах предыдущей судебной практики. В конечном итоге такие технологии сокращают трудозатраты и повышают эффективность и качество работы

юристов, снижая издержки клиента и экономя время специалиста.

Однако на этом направлении внедрения Legal Tech возникают проблемы, связанные с самостоятельностью профессионального юриста. Использование информационных технологий, автоматизирующих процесс принятия решений, не вызывает возражений только в том случае, если процесс оценки и его конечный результат осознается юристом, ведущим дело. Предоставление клиенту рекомендаций, не основанных на собственном понимании обстоятельств дела и применимых норм права, может рассматриваться как нарушение профессиональной этики.

Отсюда возникает еще одна проблема: смогут ли молодые практикующие юристы беспроблемно и быстро перестроиться на использование Legal Tech в своей деятельности так, чтобы у потребителя (клиента) не возникал вопрос о профпригодности специалиста? В результате активной информатизации быстрыми темпами растет спрос на юристов, владеющих навыками работы с информационными технологиями. Необходимо внедрять в образовательную программу дисциплины, направленные на развитие аналитического склада ума у юных специалистов и приобщать их к использованию Legal Tech с первых курсов обучения. Это позволит нам справляться с конкуренцией на быстрорастущем рынке юридических

услуг и упрочить нашу профпригодность.

3. Повышение эффективности правосудия:

Новые технологии можно использовать также для повышения эффективности работы судей. Эти инструменты помогут выделить ключевые моменты и правовые вопросы спора, а также позволят найти решения по похожим делам для повторного использования.

Активное использование ИТ в юриспруденции может разрешить множество проблем, связанных с загруженностью работы судей. Ханлар Джафарович Аликперов, специалист по уголовному праву и криминологии, доктор юридических наук, высказывает мысль о том, что человек, осуществляющий правосудие, не способен выносить справедливые решения по конкретным делам ввиду его субъективного мышления и сознания. Он предложил использовать программу автоматического определения меры наказания, заменяя возможный непрофессионализм человека на устойчивую автоматизированную машину³.

Кроме того, уже известны случаи использования электронного судьи в Эстонии. Роботы-судьи рассматривают гражданские споры на суммы до 7 тыс. евро, анализируя представленные в электронном виде документы сторон и вынося по ним взвешенное решение.

Но можно ли доверять искусственному интеллекту

вынесение судебных решений по разным категориям дел? Частично. Я не считаю возможным применять роботов-судей при разрешении уголовных дел, гражданских дел, связанных со спором о детях, дел, связанных с государственной и иной тайнами. Это связано с риском несоблюдения роботом одного из основных принципов уголовного права, закрепленного в статье 6 УК РФ, – справедливости. Увы, машина не способна в полной мере оценить все обстоятельства по делу и учитывать их при вынесении приговора. Решение дел, связанных с детьми, также требует особого внимания к мелким, на первый взгляд, деталям. Решение судьи в данных делах может определить дальнейшую жизнь человека, поэтому довольно негуманно перекладывать ответственность за жизнь других людей на робота. Действительно, электронные судьи могут существенно разгрузить работу судов первой инстанции, разрешая наиболее простые дела, выполняя, по сути, работу мировых судей, заменяя их.

Активное распространение и использование Legal Tech вызывает беспокойство о перспективах замены профессии юриста, однако предсказать, насколько существенным это влияние будет в длительной перспективе, сложно.

Исходя из данных 2017 г., Сбербанк одним своим внедрением робота-юриста, который пишет исковые заявления по физическим лицам, смог освободить около 3000

³ Аликперов Х. Д. Электронная система определения оптимальной меры наказания (постановка проблемы) // Криминология:

вчера, сегодня, завтра. 2018. № 4 (51). С. 13–22.

рабочих мест по юридической специальности. Эти цифры действительно настораживают. Позиция Германа Оскаровича Грефа, председателя правления «Сбербанка России», отчетливо прослеживается в его высказывании о том, что современным компаниям не нужны юристы без знаний в области искусственного интеллекта и понимания работы современных компьютерных технологий. С одной стороны, мы видим угрозу в перспективном «отмирании» профессии юриста в том смысле, в каком мы привыкли ее понимать. Но, с другой стороны, эта ситуация выглядит как повод для приобретения действующими юристами новых навыков работы с IT, а также как необходимость перестраивания учебного процесса в юридических высших учебных заведениях в сторону информатизации.

Вопрос об исчезновении профессии юриста в перспективе хотя и имеет за собой определенные основания, однако может опровергаться наличием у юриста Soft Skills, позволяющих ему успешно выступать на судебных заседаниях, защищая собственную позицию.

Soft Skills – это навыки, не связанные со знанием правовых норм, это умение грамотно выстраивать свою речь, защищать позицию, презентовать себя. Данные навыки отличают юриста от Legal Lech и являются одним из основных критериев оценки деятельности профессиональных специалистов, позволяя наилучшим образом фиксировать риски процесса на основе

интерпретации существующего законодательства.

В соответствии со статьей 12 ГПК РФ предполагается состязательность и равноправие сторон в гражданском процессе. Интересы сторон, как правило, представляют профессиональные юристы, деятельность которых направлена на защиту частных интересов. Legal Tech, увы, не способен заменить юриста в этом плане, однако его инструменты позволяют существенно упростить черновую работу специалиста.

В этом, по моему мнению, и заключается основная задача всей IT-сферы. Такая автоматизация юридической деятельности в совокупности с профессиональной деятельностью юриста позволяет существенно облегчить его работу, позволяя ему впоследствии лучше углубиться в правовую специфику конкретного юридического спора, сконцентрироваться на той части бумажной работы, которая действительно требует высокой степени интеллектуальной вовлеченности.

Всю совокупность рутинной работы будет выполнять автоматизированный механизм, не допускающий ошибок в заполнении документов, поиске необходимой информации, а представлять доверителя в суде, формулировать правовую позицию клиентов, вести с ними переговоры – прерогатива высококвалифицированного юриста.

Данные положения наталкивают на мысль о том, что на данный момент отсутствуют какие-либо основания полагать, что профессия юриста

перестанет быть востребованной и в ближайшее время исчезнет с рынка трудовых услуг. Legal Tech существенно снижает нагрузку юриста, не заменяя его, а лишь дополняя, совершенствуя его

деятельность, являясь его главным помощником в подготовке юридических актов, формализации исков, апелляционных, кассационных и надзорных жалоб.

Список литературы

1. Аликперов Х. Д. Электронная система определения оптимальной меры наказания (постановка проблемы) // Криминология: вчера, сегодня, завтра. 2018. № 4 (51). С. 13–22.
2. Кузнецов А. Словарь юриста: Legaltech, Lawtech и Regtech [Электронный ресурс] // RUSBASE. 2019. 12 марта. URL: <https://rb.ru/story/law-dictionary/>.
3. Михайлова А. Юридический баттл: робот от МегаФон vs Роман Бевзенко // Право.Ру. 2018. 17 мая. URL: <https://pravo.ru/lf/story/202675/>.
4. Рожкова М. А. LegalTech и LawTech – что это такое и в чем их значимость для права? // Закон.ру. 2020. 14 фев. URL: https://zakon.ru/blog/2020/02/14/legaltech_i_lawtech_-%C2%A0что_ето_такое_i_v_chem_ih_znachimost_dlya_prava.

Leonid S. Krut

Student,

Ural State Law University
(Yekaterinburg, Russian Federation)
leonidkrut3002@gmail.com

Scientific supervisor – E. V. Dzhenakova, Senior Lecturer of the Department of Information Law

LEGAL TECH: A FRIEND OR ENEMY OF A LAWYER?

Abstract: With the development of technology and the constant change in social life, adjustments are being made to our professional sphere. New technologies are emerging that, with their capabilities and innovations, at first glance, tend to devalue the legal profession. The functions of the new robots, the purpose of which is to provide legal assistance and consultation to the population through a direct analysis of the norms of law and legal practice, not only coincide with the functions of our profession, but also substantially complement them, guiding us in solving legal problems with the help of formal norms determined by the legislation of that or another country.

As a result, the question arises about the popularity and relevance of these IT technologies in the legal services market, as well as the prospect of the disappearance of the legal profession in the future. The introduction of specialized machines and tools into the daily routine work increases competition within our profession and creates additional conditions, requirements, young lawyers without following them simply cannot reveal

their professional aptitude. This issue stands squarely in discussions with prominent lawyers of our time. So, in 2018, the real duel of R.S. Bevzenko with a robot developed on the basis of neural networks using data sets including court practice, business correspondence, scientific papers and legal positions of lawyers. A well-known practicing lawyer won the sensational debate, but the debate about the possibilities of robots in jurisprudence has not subsided to this day.

Keywords: Legal tech, informatization in jurisprudence, electronic judge, computer technologies in jurisprudence, automation of legal activity.

Раздел VII

КИБЕРПРЕСТУПНОСТЬ, ТЕХНОЛОГИИ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Зуев Сергей Васильевич

Доктор юридических наук, заведующий кафедрой правоохранительной
деятельности и национальной безопасности,
Южно-Уральский государственный университет
(г. Челябинск, Российская Федерация)
zuevsergej@inbox.ru

КРИЗИС СЛЕДСТВЕННОЙ ВЛАСТИ И ПЕРЕХОД НА ЦИФРОВОЕ ДОСУДЕБНОЕ ПРОИЗВОДСТВО ПО УГОЛОВНЫМ ДЕЛАМ

Аннотация: В статье автор утверждает, что органы предварительного расследования в настоящее время переживают далеко не самые лучшие времена. Можно говорить о кризисе следственной власти в России. Представляется, что кардинально изменить ситуацию может переход на цифровую форму досудебного производства. Для этого необходимо выполнить ряд условий: установить обязательную подачу заявления о преступлении в электронном виде; создать единую цифровую платформу фиксации всего производств по делу; широко применять дистанционные формы проведения процессуальных действий; внедрить электронное взаимодействие всех участников процесса; создать доступную (комфортную) среду для лиц, участвующих в цифровом досудебном производстве.

Ключевые слова: досудебное производство, кризис, цифровизация, электронный документооборот, расследование, электронное уголовное дело.

Для цитирования:

Зуев С. В. Кризис следственной власти и переход на цифровое досудебное производство по уголовным делам // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 315–318.

Анализ состояния дел позволяет утверждать, что на сегодня органы предварительного расследования, прежде всего относящиеся к системе МВД России, переживают далеко не самые лучшие времена. С уверенностью можно говорить о кризисе следственной власти, на что указывает ряд факторов.

Кадровый голод. Низкоквалифицированный состав следователей, большая загруженность. Квалифицированных специалистов для работы в

следственных подразделениях катастрофически не хватает, особо нет и желающих поступать на службу. Кадровый вопрос решается за счет привлечения выпускников вузов, которые после непродолжительного времени увольняются. Их не устраивают условия работы и оплата труда, график, постоянные сверхурочные часы, которые сводят на нет их личную жизнь. Это является результатом того, что сотрудники долго не задерживаются, увольняются, не успевают приобрести

профессиональный опыт, не заинтересованы в повышении квалификации, не мотивированы на качественный результат своей работы.

По результатам исследования социологов К. Титаева и М. Шклярук¹ средний возраст следователя – 31–33 года, средний стаж следователя в МВД составляет около 10 лет; в производстве следователя одновременно находится 13,1 дел; почти 40 % следователей получили заочное образование. В Следственном Комитете России наблюдается гигантская текучка: до половины его сотрудников имеет опыт работы менее трех лет. Соответственно люди не успевают приобрести должную квалификацию, что, безусловно, сказывается на качестве расследования преступлений, в том числе важных и резонансных криминальных событиях².

Недостаточное материальное обеспечение. Уже на протяжении десятка лет денежное довольствие следователей не менялось. При этом увеличивается несоответствие физических и психологических затрат материальному вознаграждению. Накопительная система взысканий не позволяет эффективно применять

стимулирующие финансовые средства в виде премирования. Материальная неудовлетворенность сказывается на результатах работы.

Постоянные нападки на органы предварительного расследования. Такие нападки просматриваются со стороны отдельных представителей государственных органов власти, а также ученых, адвокатов. В литературе, в социальных сетях, в СМИ можно встретить предложения по ликвидации досудебного производства³, передачи части полномочий институту следственных судей⁴, переложение ответственности (в том числе материальной) на следователей за реабилитационный акт, полученный в суде по результатам рассмотрения уголовного дела⁵.

Отсутствие надлежащих технических средств обеспечения расследования преступлений. Во многих случаях отсутствие необходимой компьютерной и оргтехники, специального оборудования, различных криминалистических средств компенсируется устаревшими методами работы. Анализ практики показывает относительно низкий

¹ Кирилл Титаев, Мария Шклярук – научные сотрудники Института проблем правоприменения при Европейском университете в Санкт-Петербурге.

² Следствие под следствием // Коммерсант. Огонёк. 2016. 3 окт. № 39. URL: <https://www.kommersant.ru/doc/3099961> (дата обращения: 29.04.2021).

³ Александров А. С. Институт следственной власти в России: краткая история возникновения, развития и дегенерации // Юридическая наука и практика. Вестник

Нижегородской академии МВД России. 2016. № 2 (34). С. 411.

⁴ Смирнов А. В. Возрождение института следственных судей в российском уголовном процессе // РАПСИ. 2015. URL: http://rapsinews.ru/judicial_analyst/20150224/273218436.html (дата обращения: 29.04.2021).

⁵ Ковтун Н. Н. Регрессный иск к следственным органам: легальное средство назначения «стрелочника», допустившего сбой в уголовно-процессуальной системе // Российский журнал правовых исследований. 2020. Т. 7, № 2. С. 93–104.

уровень готовности использования результатов достижениями современной науки и техники среди личного состава следственных органов.

По мнению указанных социологов, следователь в России очень сильно перегружен ненужной работой. Ему некогда вникать в сложные дела, так как от этого могут пострадать показатели работы или ему придется потратить дополнительное время. Русская традиция требует оформления огромного количества бумаг по очень простым преступлениям⁶.

Представляется, что кардинально изменить ситуацию может переход на цифровую форму досудебного производства по уголовным делам. Кризис следственной власти можно рассматривать как положительный аргумент к актуализации вопроса о масштабном реформировании существующей системы расследования преступлений. И здесь следует учитывать некоторые

обязательные условия переходу на цифровой формат.

1. Обязательная подача заявления о преступлении в электронном виде.

2. Создание единой цифровой платформы фиксации всего производства по уголовным делам.

3. Широкое применение дистанционных форм проведения процессуальных действий.

4. Внедрение электронного взаимодействия всех участников процесса относительно конкретного уголовного дела, включая контроль и надзор за соблюдением законности.

5. Создание доступной (комфортной) среды для лиц, участвующих в досудебном производстве, с развитой системой электронного документооборота.

Таким образом, кризис следственной власти может быть преодолен благодаря широкому внедрению цифровых технологий в досудебное производство по уголовным делам, включая так называемое «Электронное уголовное дело».

Список литературы

1. Александров А. С. Институт следственной власти в России: краткая история возникновения, развития и дегенерации // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2016. № 2 (34). С. 405–411.

2. Ковтун Н. Н. Регрессный иск к следственным органам: легальное средство назначения «стрелочника», допустившего сбой в уголовно-процессуальной системе // Российский журнал правовых исследований. 2020. Т. 7, № 2. С. 93–104.

3. Смирнов А. В. Возрождение института следственных судей в российском уголовном процессе // РАПСИ. 2015. URL: http://rapsinews.ru/judicial_analyst/20150224/273218436.html.

⁶ Следствие под следствием // Коммерсант. Огонёк. 2016. 3 окт. № 39. URL:

<https://www.kommersant.ru/doc/3099961> (дата обращения: 29.04.2021).

Sergey V. Zuev

Doctor of Law, Head of the Department of Law Enforcement and National Security,
South Ural State University
(Chelyabinsk, Russian Federation)
zuevsergej@inbox.ru

CRISIS OF THE INVESTIGATIVE POWER AND THE TRANSITION TO DIGITAL PREDICTION PROCEEDINGS IN CRIMINAL CASES

Abstract: In the article the author argues that the preliminary investigation bodies are currently experiencing far from the best of times. We can talk about a crisis of investigative power in Russia. It seems that the transition to a digital form of pre-trial proceedings can dramatically change the situation. For this it is necessary to fulfill a number of conditions: to establish mandatory electronic filing of a crime report; to create a single digital platform for fixing all proceedings on the case; to widely use remote forms of procedural actions; to introduce electronic interaction of all participants in the process; to create an accessible (comfortable) environment for persons involved in digital pre-trial proceedings.

Keywords: pre-trial proceedings, crisis, digitalization, electronic document management, investigation, electronic criminal case.

УДК 343.98

Степаненко Диана Аркадьевна

Доктор юридических наук, профессор, профессор
кафедры криминалистики, судебных экспертиз и юридической психологии
Института государства и права,
Байкальский государственный университет
(г. Иркутск, Российская Федерация)
diana-stepanenko@mail.ru

Рудых Алексей Александрович

Кандидат юридических наук,
отдел «К» (по борьбе с правонарушениями в сфере информационных технологий)
ГУ МВД России по Иркутской области
(г. Иркутск, Российская Федерация)
irkutianin38@gmail.com

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ МЕХАНИЗМА УДАЛЕННОЙ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация: В статье рассматриваются вопросы, касающиеся использования информационных технологий для осуществления правоохранительной деятельности в дистанционном формате. Авторы обращают внимание на недостаточную эффективность существующих способов осуществления расследования в условиях роста количества дистанционных преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Обращено внимание на проблему удостоверения личности и полномочий пользователей в рамках удаленного взаимодействия. Предлагается к исследованию возможность вовлечения в поле правоохранительной деятельности существующих систем: единой системы идентификации и аутентификации и единой биометрической системы. Описаны возможности использования дополнительных методов аутентификации пользователей.

Ключевые слова: дистанционный, аутентификация, преступление, идентификация, биометрический, информационные технологии, дистанционный формат.

Для цитирования:

Степаненко Д. А. К вопросу об использовании механизма удаленной идентификации и аутентификации в правоохранительной деятельности / Д. А. Степаненко, А. А. Рудых // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 319–327.

В условиях динамичного развития информационных технологий, пандемия, вызванная распространением вируса covid-19, оказалась фактором, провоцирующим ускорение внедрения различных видов онлайн-взаимодействия между людьми.

Введенные ограничения предопределили, в том числе, и процессы преобразования многих «контактных» преступлений в дистанционный формат их совершения. Мы наблюдаем как способы подготовки, совершения и сокрытия преступления в результате встраивания в его функциональную составляющую информационных технологий претерпевают трансформации, что не осталось без внимания исследователей¹. Преступники активно используют различные виды технологий обработки компьютерной информации, тем самым усиливая «эффективность» криминальной деятельности.

В последнее время, отмечен существенный рост преступлений, совершенных с использованием информационных технологий, в которых последние используются, как коммуникативно-координирующая основа. Доля в структуре общей преступности подобных преступлений составляет уже более четверти².

Одним из проявлений информационных технологий в

механизме преступления является возможность его совершения дистанционно. При таком способе преступник не ограничен территорией своего физического пребывания и способен совершать преступления в отношении широкого круга лиц, находящихся в любом другом месте, как на территории нашей страны, так и за ее пределами.

Сегодня существенная часть преступлений в сфере незаконного оборота наркотических средств и мошенничеств совершается дистанционным способом. Кроме того, не обошел стороной дистанционный способ совершения и преступления против половой неприкосновенности несовершеннолетних. Одним словом, все больше видов криминальных деяний сегодня совершаются с использованием цифровых дистанционных технологий.

В свою очередь, такие изменения создают ряд затруднений в деятельности правоохранительных органов. Это связано с тем, что в организационной основе осуществления уголовно-процессуальной и оперативно-розыскной деятельности предусмотрен территориальный принцип работы, что закреплено в ряде нормативных актов.

¹ Степаненко Д. А. Киберпространство как модулятор процесса расследования преступлений и развития криминалистической науки // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 1 (27). С. 81.

² Краткая характеристика состояния преступности в Российской Федерации за январь–февраль 2021 года // Министерство внутренних дел РФ: официальный сайт. URL: <https://xn--b1aew.xn--p1ai/reports/item/23447482/> (дата обращения: 05.04.2021).

Так, в соответствии с ч. 3 ст. 25 Федерального закона «О полиции»³, сотрудник полиции осуществляет свои права и выполняет обязанности в пределах территории, которую обслуживает орган внутренних дел, в котором он проходит службу.

Кроме того, по общему правилу в соответствии с ч. 1 ст. 152 УПК РФ предварительное расследование осуществляется по месту совершения преступления.

Однако, при совершении дистанционных преступлений определить место совершения удастся не всегда, следовательно, расследование осуществляется по месту выявления признаков преступления.

Существующая нормативная база все же предусматривает возможности осуществления следственных действий или оперативно-розыскных мероприятий за пределами территории, обслуживаемой органом внутренних дел. Как правило, такие способы решения правоохранительных задач реализуются в форме служебных выездов, организации служебных командировок, направлении письменных поручений о производстве отдельных

следственных действий и проведении оперативно-розыскных мероприятий.

Перечисленные способы правоохранительной работы, по своей сути, являются контактными, где информационно-телекоммуникационная составляющая сведена к минимуму. Такие способы не отвечают современным требованиям к эффективности и имеют свои недостатки, на которые указывают авторы⁴.

Ограничения в деятельности субъектов расследования, обусловленные территорией обслуживания и контактным способом работы, создают последним потенциально «невыгодные» условия, в отличие от преступников, совершающих экстерриториальные преступления в сфере информационных технологий, на что мы ранее уже обращали внимание⁵.

Указанные проблемы расследования дистанционных преступлений исследовались отдельными авторами⁶. Кроме того, рядом авторов поднимались вопросы отсутствия механизмов дистанционной работы со следовой информацией. В частности, А. И. Иванов, высказывает сожаление по поводу отсутствия правовых норм,

³ О полиции: федеральный закон от 07.02.2011 № 3-ФЗ (последняя редакция) // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_110165/ (дата обращения: 05.04.2021).

⁴ Фисаков М. Ю. Перспективы использования информационно-коммуникационных технологий в деятельности следователей // Философия права. 2020. № 4 (95). С. 112.

⁵ Рудых А. А. О некоторых направлениях цифровизации расследования преступлений

// Сибирские уголовно-процессуальные и криминалистические чтения. 2019. № 3 (25). С. 73.

⁶ Костенко Н. С., Семенов Г. М., Пшеничкин А. А. Основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, на современном этапе // Вестник Воронежского института МВД России. 2020. № 4. С. 193.

регламентирующих процедуры дистанционного исследования компьютерной информации, что ограничивает деятельность субъекта расследования⁷.

В свете осознания этих проблем, особенно актуально звучит заявление президента РФ В. В. Путина, который, выступая на расширенном заседании коллегии МВД России 3 марта 2021 года, отметил, что сегодня необходимо внедрять дистанционные технологии осуществления правоохранительной деятельности⁸.

В настоящее время исследователи темы информационных технологий в юридической деятельности рассматривают их, в том числе, как инструмент оптимизации юридической деятельности, а также как приемы и способы работы со следовой информацией⁹.

Анализ проблематики указанного направления показывает, что на сегодняшний день уже существуют примеры внедрения дистанционных способов взаимодействия в различных сферах для осуществления юридически значимых действий.

Так, сегодня с использованием платформы государственных услуг, можно дистанционно зарегистрировать юридическое лицо, направить в налоговые органы отчетность, открыть банковский счет, направить исковое заявление в суд и прочее.

В частности, в конце 2020 года в рамках развития цифрового нотариата вступили в силу поправки, введенные Федеральным законом № 480-ФЗ¹⁰.

Согласно нововведениям, у нотариусов появилась возможность удостоверения сделок дистанционным способом с участием двух и более лиц без их совместного присутствия у одного и того же нотариуса.

Также законом предусмотрен ряд других новшеств, в частности, возможность установления нотариусом личности физического лица посредством доступа к единой биометрической системе, возможность направления документа в электронном виде с исполнительной надписью нотариуса в адрес судебных приставов. Указанные нововведения создадут благоприятные условия для

⁷ Иванов А. И. Удаленное исследование компьютерной информации: уголовно-процессуальные и криминалистические проблемы // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2009. Т. 9, № 2. С. 77.

⁸ Аскерова Т. А. В России могут появиться новые формы сбора доказательств по уголовным делам // Парламентская газета. 2021. 3 мар. URL: <https://www.pnp.ru/politics/v-rossii-mogut-poyavitsya-novye-formy-sbora-dokazatelstv-po-ugolovnym-delam.html> (дата обращения: 23.04.2021).

⁹ Бахтеев Д. В. Современные технологии как предмет изучения и инструмент в

юридических исследованиях и юридической деятельности // Технологии XXI века в юриспруденции: материалы Второй международной научно-практической конференции (22 мая 2020 года). Екатеринбург, 2020. С. 24.

¹⁰ О внесении изменений в Основы законодательства Российской Федерации о нотариате и отдельные законодательные акты Российской Федерации: федеральный закон от 27.12.2019 № 480-ФЗ (последняя редакция) // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_341788/ (дата обращения: 23.04.2021).

работы нотариата и предоставления нотариальных услуг гражданам.

По нашему мнению, дистанционные технологии осуществления правоохранительной деятельности, также являются в настоящее время насущной необходимостью.

Например, сегодня повысить эффективность противодействия преступности в сфере информационных технологий помогут выработанные алгоритмы производства удаленного допроса свидетеля или потерпевшего, дистанционного проведения очных ставок, осуществления дистанционных опросов различных лиц и осмотров сетевых ресурсов или электронных носителей информации и других необходимых действий.

Учитывая, что деятельность правоохранительных органов по расследованию противоправных деяний, в значительной степени, затрагивает права и законные интересы широкого круга лиц, дистанционный формат сбора

доказательств и взаимодействия с участниками уголовного судопроизводства должен основываться на принципах достоверности, законности и соблюдения всех необходимых подтверждающих процедур.

Анализ вопросов связанных с разработкой алгоритмов отдельных направлений правоохранительной деятельности в дистанционном формате выводит на первое место проблемы удостоверения личности и полномочий лиц, взаимодействующих друг с другом удаленно, а точнее вопросы идентификации¹¹ и аутентификации¹².

Для обеспечения достоверности и доступности такой деятельности, на наш взгляд, необходима разработка вопросов использования возможностей существующих систем удаленной идентификации и аутентификации.

Так, в соответствии с постановлением Правительства Российской Федерации № 977¹³ создана и функционирует Единая

¹¹ Идентификация – действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

¹² Аутентификация – действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации.

¹³ О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем,

используемых для предоставления государственных и муниципальных услуг в электронной форме» (вместе с Требованиями к федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»): постановление Правительства РФ от 28.11.2011 № 977 (ред. от 23.12.2020) // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_122455/2f48be3e2ca5e55d29265d66094

система идентификации и аутентификации (далее ЕСИА). Данная система в настоящее время используется для предоставления государственных услуг в электронном виде. Она обеспечивает процесс санкционированного доступа пользователей государственных и иных информационных систем. ЕСИА обеспечивает авторизацию на сетевых ресурсах «Госуслуги» и «Российская общественная инициатива».

Кроме того, уже сегодня создана Единая биометрическая система (далее – ЕБС), которая предназначена для аутентификации пользователей по биометрической информации. Федеральным законом от 29 декабря 2020 г. № 479-ФЗ¹⁴ ЕБС присвоен статус государственной информационной системы.

Возможности системы позволяют использовать ее для оказания дистанционных финансовых услуг. Для удостоверения личности пользователя ЕБС использует два параметра одновременно: распознавание лица и голоса.

Для повышения достоверности процедуры аутентификации в будущем возможно применение большего числа методов биометрического удостоверения личности.

Так, сегодня известны динамические и статические методы аутентификации. К последним относятся: аутентификация по

отпечатку пальца; аутентификация по сетчатке глаза; аутентификация по радужной оболочке глаза; аутентификация по геометрии руки; аутентификация по термограмме лица. К динамическим, относятся методы аутентификации по голосу и почерку.

Использование технологической базы указанных систем, по нашему мнению, возможно и в сфере осуществления правоохранительной деятельности в дистанционном формате. А удостоверение личности с использованием комплекса биометрической аутентификационной информации представляется надежным в сравнении с использованием процессуальных документов и документов, удостоверяющих личность на бумажных носителях. Примечательно, что отдельные авторы в своих исследованиях признают бумажный тип документирования в уголовном процессе как архетип¹⁵.

Кроме того, сегодня нет необходимости в разворачивании дорогостоящей системы специальной связи, оборудования помещений и обучения персонала для реализации дистанционных процедур в сфере правоохранительной деятельности.

Персональные электронные устройства субъекта расследования и любых других лиц, при наличии специально разработанного программного приложения, способны

f394b5a385961/ (дата обращения: 23.04.2021).

¹⁴ О внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 29 декабря 2020 г. № 479-ФЗ // СПС «Консультант Плюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_372645/ (дата обращения: 23.04.2021).

¹⁵ Зуев С. В. Цифровая среда уголовного судопроизводства: проблемы и перспективы // Сибирский юридический вестник. 2018. № 4 (83). С. 120.

обеспечить выполнение необходимых алгоритмов. О возможности повышения эффективности расследования и раскрытия преступлений путем использования персональных электронных мобильных устройств неоднократно указывалось ранее¹⁶.

Устройства, которые имеются в пользовании у каждого человека, уже обладают необходимым функционалом для обеспечения процедуры многофакторной аутентификации. В составе большинства современных устройств имеются такие модули как: микрофон, воспринимающий речь, камера, сканер отпечатков пальцев. Это позволяет воспринимать и использовать необходимые аутентификационные биометрические данные для процедур удостоверения подлинности личности пользователя.

Разработка направления использования систем идентификации и аутентификации приобретает еще большую актуальность в свете приближающегося внедрения электронных паспортов граждан РФ.

Так, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации уже представило проект Указа Президента РФ «О паспорте гражданина Российской Федерации, содержащем электронный носитель информации»¹⁷.

Согласно проекту, предлагается уже с 1 декабря 2021 года на территории г. Москвы и до 1 июля 2023 года на территории Российской Федерации, начать выдачу паспортов гражданам РФ с электронным носителем информации. Указанный электронный носитель будет содержать биометрические данные владельца паспорта, в том числе изображение его лица и папиллярных узоров двух пальцев рук.

Также к использованию предлагается мобильный идентификатор гражданина, который представляет собой программное приложение на смартфон, которое будет выполнять функции паспорта.

Электронные паспорта с биометрической информацией о владельце, по нашему мнению, могут стать важным элементом процедур аутентификации и идентификации личности в рамках разработанных в будущем алгоритмов дистанционного осуществления правоохранительной деятельности.

По нашему мнению, исследование вопросов применения систем идентификации и аутентификации, а также использования электронных идентификаторов личности как основы дистанционного формата правоохранительной работы позволит субъектам расследования повысить эффективность противостояния

¹⁶ Беляков А. А., Бахтеев Д. В. Мобильный справочник следователя: содержание и технические условия разработки // Технологии XXI века в юриспруденции: материалы Всероссийской научно-практической конференции (24–25 мая 2019 года) / под ред. Д. В. Бахтеева. Екатеринбург, 2019. С. 24.

¹⁷ О паспорте гражданина Российской Федерации, содержащем электронный носитель информации: проект Указа Президента РФ. ID проекта 04/14/03-21/00114294, подготовлен Минцифры России // СПС «Консультант Плюс».

экстерриториальной преступности в
сфере информационно-
телекоммуникационных технологий.

Список литературы

1. Бахтеев Д. В. Современные технологии как предмет изучения и инструмент в юридических исследованиях и юридической деятельности // Технологии XXI века в юриспруденции: материалы Второй международной научно-практической конференции (Екатеринбург, 22 мая 2020 года) / под ред. Д. В. Бахтеева. Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2020. С. 23–29.
2. Беляков А. А. Мобильный справочник следователя: содержание и технические условия разработки / А. А. Беляков, Д. В. Бахтеев // Технологии XXI века в юриспруденции: материалы Всероссийской научно-практической конференции (Екатеринбург, 24–25 мая 2019 года) / под ред. Д. В. Бахтеева. Екатеринбург: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет», 2019. С. 23–26.
3. Зуев С. В. Цифровая среда уголовного судопроизводства: проблемы и перспективы // Сибирский юридический вестник. 2018. № 4 (83). С. 118–123.
4. Иванов А. И. Удаленное исследование компьютерной информации: уголовно-процессуальные и криминалистические проблемы // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2009. Т. 9, № 2. С. 75–77.
5. Костенко Н. С. Основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, на современном этапе / Н. С. Костенко, Г. М. Семенов, А. А. Пшеничкин // Вестник Воронежского института МВД России. 2020. № 4. С. 192–196.
6. Рудых А. А. О некоторых направлениях цифровизации расследования преступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2019. № 3 (25). С. 70–79.
7. Степаненко Д. А. Киберпространство как модулятор процесса расследования преступлений и развития криминалистической науки // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 1 (27). С. 77–88.
8. Фисаков М. Ю. Перспективы использования информационно-коммуникационных технологий в деятельности следователей // Философия права. 2020. № 4 (95). С. 109–112.

Diana A. Stepanenko

Doctor of Law, Professor, Professor of the
Department of Criminalistics, Forensic Examinations and Legal Psychology,
Institute of State and Law,
Baikal State University
(Irkutsk, Russian Federation)
diana-stepanenko@mail.ru

Alexey A. Rudykh

PhD (Law),
Department "K" (for the fight against offenses in the field of information technology) of
the Main Directorate of the Ministry of Internal Affairs of Russia for the Irkutsk Region
(Irkutsk, Russian Federation)
irkutianin38@gmail.com

THE QUESTION OF USING THE REMOTE IDENTIFICATION AND AUTHENTICATION MECHANISM IN LAW ENFORCEMENT

Abstract: The article discusses issues related to the use of information technology for the implementation of law enforcement in a remote format. The authors draw attention to the insufficient effectiveness of existing methods of investigating in the face of an increase in the number of remote crimes committed using information and telecommunication technologies. Attention is drawn to the problem of identity and user authority within the framework of remote interaction. It is proposed to study the possibility of involving existing systems in the field of law enforcement: a unified identification and authentication system and a unified biometric system. Possibilities of using additional methods of user authentication are described.

Keywords: remote, authentication, crime, identification, biometric, information technology, remote format.

УДК 343.98

Дерюгин Роман Александрович

Кандидат юридических наук, заместитель начальника кафедры криминалистики,
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
deryugin.r.a@mail.ru

Феклушина Анастасия Алексеевна

Курсант, рядовой полиции,
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
lucky_girl_kate@mail.ru

**О НЕКОТОРЫХ ВОПРОСАХ, СВЯЗАННЫХ С РАССЛЕДОВАНИЕМ
ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ПРИМЕНЕНИЕМ МЕТОДОВ
СОЦИАЛЬНОЙ ИНЖЕНЕРИИ**

Аннотация: Автор проанализировал статистику по количеству преступлений, совершенных с использованием информационно-телекоммуникационных технологий, а также некоторые причины роста киберпреступлений. В статье рассмотрены самые распространенные виды фишинга, применяемые преступниками в настоящее время, и проблемы, связанные с расследованием преступлений, совершенных с применением методов социальной инженерии.

Ключевые слова: информационно-телекоммуникационные технологии, фишинг, социальная инженерия, киберпреступления.

Для цитирования:

Дерюгин Р. А. О некоторых вопросах, связанных с расследованием преступлений, совершенных с применением методов социальной инженерии / Р. А. Дерюгин, А. А. Феклушина // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 328–335.

Становление информационного общества и стремительные темпы развития информационно-телекоммуникационных технологий точно характеризуют 21 век и современный мир. Использование интернет-банкинга, интернет-магазинов, широкого перечня услуг операторов связи, сервисов безналичных платежей,

бесконтактной оплаты и доставки, облачных хранилищ, сервисов и стало обыденным и привычным в жизни каждого человека и видится как неотъемлемая часть повседневной деятельности людей. Перечисленные технологии и онлайн-услуги были и остаются популярными, а во время пандемии ускорили свое развитие и продолжают совершенствоваться. По

данным компании DataInsight, чаще раза в месяц до пандемии в интернете что-то покупали 43 процента респондентов. За две недели с начала пандемии сделали покупки более 80 %. С началом самоизоляции выросла доля онлайн-покупок продуктов. Большинство российских интернет-пользователей (67 %) за время самоизоляции совершали покупки онлайн, а каждый четвертый (26 %) заказывал доставку продуктов питания на дом, показало совместное исследование Роскачества и Аналитического центра НАФИ¹. Несмотря на преимущественно положительный аспект развития указанных технологий, именно в период пандемии выросло число киберпреступлений. Очевидно, что работа в удаленном режиме увеличила количество потенциальных жертв киберпреступлений, особенно мошенничеств.

Киберпреступники расширили криминальную деятельность, чтобы использовать социальные, юридические и психологические нюансы, связанные с COVID-19. Так, за 2020 год число преступлений, совершенных с использованием информационно-телекоммуникационных технологий,

возросло на 73,4 %, в том числе с использованием сети Интернет – на 91,3 %, при помощи средств мобильной связи – на 88,3 %². К сожалению, тенденции роста не снижаются. Кроме того, в первом квартале текущего года в IT-сфере совершено на 33,7 % больше преступлений, чем год назад, в том числе с использованием сети Интернет – на 51,6 % и при помощи средств мобильной связи – на 31,6 %. В январе–марте 2020 года удельный вес таких деяний составлял 19,9 % от общего числа зарегистрированных преступлений, а за три месяца 2021 года увеличился до 27,1 %³. Статистические показатели свидетельствуют об увеличении преступлений указанной категории в разы.

С учетом глобализации общества жертвами таких преступлений становятся не только отдельные граждане, но и целые государства. В связи с этим, согласимся со словами бывшего руководителя Интерпола Хунвэя: «Сейчас мы стоим перед новым, виртуальным миром преступлений, которые имеют трансграничный, стремительно нарастающий характер»⁴.

¹ Онлайн-покупки останутся популярными и после пандемии // Российская газета. 2020. 13 мая. URL: <https://rg.ru/2020/05/13/onlajn-pokupki-ostanutsia-populiarnymi-i-posle-randemii.html> (дата обращения: 15.05.2021).

² Состояние преступности в России за январь–декабрь 2020 года: сборник статистики и аналитики МВД России // Министерство внутренних дел РФ: официальный сайт. URL: <https://мвд.рф/reports/item/22678184/> (дата обращения: 15.05.2021).

³ Состояние преступности в России за январь–март 2021 года: сборник статистики и аналитики МВД России // Министерство внутренних дел РФ: официальный сайт. URL: <https://мвд.рф/files/application/2111940> (дата обращения: 15.05.2021).

⁴ Мир не может эффективно бороться с киберпреступлениями, заявили в Интерполе // РИА новости. 2018. 6 июля. URL: <https://ria.ru/20180706/1524100913.html> (дата обращения: 13.05.2021).

Вышесказанное подтверждает актуальность исследований, посвященных вопросам, связанным с расследованием киберпреступлений, и обуславливает необходимость рассмотрения некоторых проблем в этой сфере, а также современных наиболее распространенных способов совершения преступлений, связанных с использованием информационно-телекоммуникационных технологий.

Большая часть преступлений, связанных с использованием информационно-телекоммуникационных технологий, совершается с применением методов социальной инженерии, который основан на доступе к компьютерной информации и данным пользователей для дальнейшего общения с ними, введения в заблуждение, получения сведений, необходимых для доступа к денежным средствам потерпевшего или прямого перевода денежных средств преступнику.

При использовании методов социальной инженерии преступники активно применяют психологические приемы воздействия на жертву (убеждение, воздействие на слабости человека, отдельные черты личности, такие как жадность, страх, безразличие, любопытство). Всем известны многочисленные примеры, когда преступник звонит потерпевшему от лица сотрудника службы безопасности банка, под различными предложениями (проверка данных о личности клиента, взлом интернет-банка, фиксация попыток списания денег с карты,

подтверждение заявки на кредит) получает пароль от личного кабинета пользователя и списывает определенную сумму денег.

Остается популярным такой вид социальной инженерии как фишинг⁵. Фишинг – создание вредоносного сайта или ссылки, по которой пользователь сталкивается с необходимостью идентификации. Например, в электронном письме вам сообщили, что ваш аккаунт в социальной сети был взломан, для его блокировки/разблокировки необходимо пройти по ссылке и авторизоваться (ввести логин, пароль или иные сведения). Цели, которые преследует такая цифровая угроза как фишинг, могут быть разными:

- персональные данные;
- сведения о логинах и пароли;
- данные карт, банковских счетов;
- конфиденциальная информация о компании и т. п.

Можно выделить несколько видов фишинга:

Классический. Представляет собой рассылку электронных писем. Программа рассылки использует данные адресов электронной почты, полученные чаще всего посредством парсинга. Парсинг – это сбор данных специальной программой из открытых источников. Обычно сообщение с признаками фишинга содержит примерно такую информацию:

- ваша учетная запись заблокирована, чтобы восстановить доступ, перейдите по ссылке;

⁵ Фишинг образовано от английского слова «phishing», которое является производным от «fishing» (ловля рыбы, рыбалка).

- для продолжения работы требуется подтвердить учетную запись;

- обнаружена подозрительная активность, рекомендуем изменить пароль;

- у вас есть важное сообщение от банка, налоговой службы, службы судебных приставов и т. п.

Обычно ссылка внизу письма ведет на вредоносный сайт, где вас попросят ввести какие-либо данные, которые необходимы мошенникам. Это могут быть пароли от аккаунтов социальных сетей, интернет-магазина, личного кабинета банка и др.

Целенаправленный фишинг. Используя данный вид фишинга, мошенники располагают уже большим объемом данных. Они могут знать ваше имя, фамилию, регион проживания, сферу деятельности и даже наименование банка, в котором открыт счет. Такие сведения собираются из открытых источников, только информация обрабатывается вручную. Текст сообщения составляется таким образом, чтобы получить доверие человека.

Получив, например, письмо от «Сбербанка» о подозрительной активности со счетом, клиент может ничего не подозревая перейти по вредоносной ссылке.

Охота на «китов». Данный вид фишинга имеет более узкое назначение. Его целью является конфиденциальная информация о бизнесе. Например, доступ к клиентской базе с контактами, применение каких-то технологий, данные об учредителях и их банковских счетах и т. д. «Китами» в данном случае являются сотрудники

компании – руководители высшего или среднего звена, владеющие информацией, которая представляет интерес для мошенников.

Рассылки, имитирующие сообщения от держателей облачных хранилищ данных. В некоторых случаях в письме содержится ссылка, где вас попросят авторизоваться для входа в Google или Яндекс. В результате могут быть похищены личные данные, которые хранятся на виртуальном диске: фото, рабочие файлы и др.

Вложения. На этот вид фишинга сейчас уже мало реагирует, поскольку большинство компьютеров оборудовано антивирусным программным обеспечением. К письму злоумышленники прикрепляют файл, при открытии которого на компьютер или смартфон устанавливается вредоносная программа. Если вы своевременно обновляете антивирус, система защиты не даст возможности нанести ущерб. Кроме того, большинство пользователей знают, что нельзя открывать вложения, полученные из неизвестных источников. Однако такое сообщение может прийти и от знакомого, чей аккаунт или адрес электронной почты был взломан. Кроме того, не стоит забывать и о том, что развитие вредоносных программ не стоит на месте.

Увеличение числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, распространение и совершенствование различных видов социальной инженерии, повлекло за собой появление многочисленных

проблем и вопросов, которые необходимо решать в целях повышения качества процесса расследования.

Во-первых, преступления в сфере информационно-телекоммуникационных технологий и киберпреступления характеризуются высоким уровнем латентности. Действительно, довольно часто на практике лица, ставшие потерпевшими, безосновательно предполагая о нераскрываемости данных преступлений, не обращаются с заявлением в органы внутренних дел или обращаются, но не могут предоставить минимальных данных (электронных следов, алгоритмов действий, сведений о точках доступа к информации, параметрах входа в сеть, учетных данных и т. п.). Данная проблема связана с низким уровнем знаний населения в области информационно-коммуникационных технологий, об основных способах мошенничества в данной сфере, о правилах обеспечения собственной информационной безопасности при работе в сети Интернет.

Проблема может быть решена путем разработки методических материалов, памяток безопасности при работе с ПК или иным устройством, имеющим доступ к сети Интернет, информирования о способах совершения тех или иных преступлений, а также о порядке действий при обнаружении признаков киберпреступления.

Во-вторых, низкий уровень квалификации сотрудников правоохранительных органов в области информационных технологий, отсутствие опыта

расследования преступлений указанной категории.

Напомним, что информационно-телекоммуникационные технологии влияют на развитие всех сфер деятельности общества, в том числе и преступную, а, соответственно, совершенствуются способы и методы совершения преступлений. Программы обучения молодых специалистов не успевают трансформироваться под новые виды преступлений в сфере информационно-телекоммуникационных технологий. Таким образом, современный преступник практически всегда на шаг впереди правоохранительной системы, а работа органов внутренних дел, к сожалению, не несет предупредительный характер, а по большей части направлена на раскрытие совершенных преступлений.

Одним из решений данной проблемы, будет разработка краткосрочных курсов повышения квалификации сотрудников, учитывающих текущее состояние и перспективы развития того или иного направления в сфере киберпреступности. Кроме того, необходимы консультации со специалистами в сфере IT-технологий, представителями операторов сотовой связи и информационных систем по актуальным вопросам, связанным с киберпреступностью. Особое внимание необходимо уделять техническому уровню подготовки специалистов в органах внутренних дел, который складывается из: физического, аппаратного, программного и криптографического

обучения. Помимо этого, в процессе подготовки кадров следует уделять особое внимание компьютерной криминалистике (форензике), а именно, методам сбора цифровых доказательств, анализу сетевого взаимодействия, изучению фреймворков, жестких дисков, цифровых устройств и другим аспектам, касающимся расследования преступлений.

В-третьих, низкий уровень оснащенности подразделений, занимающихся раскрытием и расследованием киберпреступлений, современными техническими средствами или отсутствие последних.

Например, средствами выемки аппаратного обеспечения и электронных доказательств; средствами создания электронных образов и хэш-кодов, восстановления данных по «отпечаткам» в памяти жестких дисков, обработки и расшифровки данных; средствами удаленной экспертизы оборудования и уничтожения информации, что свидетельствует о необходимости увеличения финансирования данной сферы в целях улучшения качества расследования компьютерных преступлений.

Четвертая проблема связана с установлением личности лица, совершившего то или иное преступление в сфере информационно-телекоммуникационных технологий с использованием незащищенных сетей (Wi-Fi сети, локальные сети предприятий, облачные хранилища и пр.).

При совершении киберпреступлений преступники, как

правило, используют «одноразовые» сим-карты, чужие устройства (мобильные телефоны, планшеты, компьютеры), анкетные данные чужих лиц, ложные аккаунты, а также другие методы скрытия следов, что в свою очередь затрудняет работу сотрудников органов внутренних дел при раскрытии и расследовании данного вида преступлений.

Решение данной проблемы лежит в разработке алгоритма действий с утраченной или потерянной информацией, в привлечении в качестве специалистов лиц, имеющих углубленные знания в данной сфере, – программистов или IT-специалистов, в качественной работе с лицами пострадавшими от киберпреступлений при допросе, а также в качественном сборе доказательств.

В качестве пятой проблемы можно выделить халатность самих пользователей, которые впоследствии оказываются потерпевшими. Пользователи вводят свои паспортные данные, данные своего аккаунта, данные банковской карты, например, при покупке через интернет-магазин, на разные незащищенные сайты, сохраняют свои учетные данные в общественных точках доступа, используют несертифицированное программное обеспечение ПК или мобильных телефонов.

Решение данной проблемы заключается в ограничении пользования незащищенными точками доступа, в использовании проверенного программного обеспечения, а также в обеспечении надлежащего функционирования сети Интернет, в мониторинге легальности

работы интернет-магазинов, а также в анализе достоверности сведений различных пользовательских сайтов.

Помимо перечисленного, в качестве проблемы можно отметить низкий уровень планирования мер, направленных на предотвращение преступлений в сети Интернет.

В связи со стремительным развитием способов и средств совершения киберпреступлений, возникает необходимость введения поправок в законодательные акты, такие как Стратегия национальной безопасности и План реализации мероприятий по ее укреплению⁶. В этих целях разработана концепция безопасного функционирования и развития сети «Интернет» (проект концепции Конвенции ООН), где приводятся принципы поведения государств по управлению глобальной сетью «Интернет» и оказанию содействия⁷.

Перечень вышеперечисленных проблем, возникающих в процессе раскрытия и расследования преступлений, совершаемых в сфере

информационно-телекоммуникационных технологий и киберпреступлений, не является исчерпывающим. Данная категория преступлений одна из самых быстроразвивающихся и требует особого внимания со стороны правоохранительных органов. Необходимо постоянное повышение квалификации и совершенствование профессиональных навыков сотрудников органов внутренних дел при работе с компьютерной техникой, устройствами связи, программным обеспечением, информационным пространством и со следами, возникающими, в связи с этим. К сожалению, статистика свидетельствует о том, что современный квалифицированный преступник не встречает должного противодействия со стороны правоохранительных органов⁸. В связи с этим данная проблема является самой главной и для повышения эффективности процесса раскрытия и расследования преступлений, требует своего разрешения.

Список литературы

1. Гончар В. В. Отдельные вопросы совершенствования подготовки кадров, специализирующихся на расследовании преступлений, совершаемых с использованием информационных технологий // Криминалистика в условиях

⁶ О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 31 декабря 2015 г. № 683 // Собрание законодательства РФ. 2016. №1. Ст. 212.

⁷ Гончар В. В. Отдельные вопросы совершенствования подготовки кадров, специализирующихся на расследовании преступлений, совершаемых с использованием информационных технологий // Криминалистика в условиях развития информационного общества (59-е

ежегодные криминалистические чтения): сборник статей Международной научно-практической конференции. Москва: Академия управления МВД России, 2018. С. 75.

⁸ Дерюгин Р. А., Файсханов И. Ф. О криминалистическом исследовании электронных носителей информации и цифровых следов // Вестник Уральского юридического института МВД России. Екатеринбург. 2019. № 4 (24). С. 64.

развития информационного общества (59-е ежегодные криминалистические чтения): сборник статей Международной научно-практической конференции. Москва: Академия управления МВД России, 2018. С. 73–77.

2. Дерюгин Р. А. О криминалистическом исследовании электронных носителей информации и цифровых следов / Р. А. Дерюгин, И. Ф. Файсханов // Вестник Уральского юридического института МВД России. Екатеринбург. 2019. № 4 (24). С. 62–65.

3. Мир не может эффективно бороться с киберпреступлениями, заявили в Интерполе // РИА новости. 2018. 6 июля.

4. Онлайн-покупки останутся популярными и после пандемии // Российская газета. 2020. 13 мая. URL: <https://rg.ru/2020/05/13/onlajn-pokupki-ostanutsia-populiarnymi-i-posle-pandemii.html>.

5. Состояние преступности в России за январь–декабрь 2020 года: сборник статистики и аналитики МВД России // Министерство внутренних дел РФ: официальный сайт. URL: <https://мвд.рф/reports/item/22678184/>.

6. Состояние преступности в России за январь–март 2021 года: сборник статистики и аналитики МВД России // Министерство внутренних дел РФ: официальный сайт. URL: <https://мвд.рф/files/application/2111940>.

Roman A. Deryugin

PhD (Law), Deputy Head of the Department of Criminalistics,
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
deryugin.r.a@mail.ru

Anastasia A. Feklushina

Cadet,
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
lucky_girl_kate@mail.ru

ABOUT SOME ISSUES RELATED TO THE INVESTIGATION OF CRIMES COMMITTED WITH THE USE OF SOCIAL ENGINEERING METHODS

Abstract: The authors analyzed statistics on the number of crimes committed using information and telecommunications technologies, as well as some reasons for the growth of cybercrime. The article discusses the most common types of phishing used by criminals at the present time, and the problems associated with the investigation of crimes committed using social engineering methods.

Keywords: information and telecommunications technologies, phishing, social engineering, cybercrime.

УДК: 343.13

Левченко Олег Викторович
Кандидат юридических наук, прокурор
Троицкого и Новомосковского
административных округов г. Москвы
(г. Москва, Российская Федерация)
2923757@rambler.ru

ПРОЦЕССУАЛЬНО-ПРАВОВАЯ ФОРМА ВЗАИМОДЕЙСТВИЯ ПРОКУРАТУРЫ И ОРГАНОВ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ ПРИ ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация: Цифровая трансформация уголовно-процессуальной системы должна происходить после проведения реформы предварительного расследования и перехода к состязательному типу уголовного судопроизводства. В новой уголовно-процессуальной модели, инсталлированной на цифровой платформе государства, прокурору надлежит занять руководящую роль в отношении органов предварительного расследования, уполномоченных на выявление, раскрытие и расследование преступлений, и принятии решении о направлении дела в суд.

Ключевые слова: прокурор, органы предварительного расследования, уголовный процесс, цифровая трансформация.

Для цитирования:

Левченко О. В. Процессуально-правовая форма взаимодействия прокуратуры и органов предварительного расследования при противодействии преступности в условиях цифровизации // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 336–344.

Нашей стране, как и другим странам мира, необходимо решить проблему модернизации национальной правоохранительной системы и процессуально-правовой формы ее деятельности по противодействию преступности в условиях цифровизации. Более всего актуализирует эту проблему рост киберпреступности, которая, по общему мнению, становится одной из главных угроз безопасности населения, бизнеса, государства.

В качестве ответной меры на данную угрозу предлагается и уже осуществляется специализация отдельных подразделений на выявление и раскрытие преступлений, совершаемых с использованием высоких технологий.

Однако, специализация сотрудников правоохранительных органов на противодействие противоправной деятельности киберпреступников, хотя и неотложная, однако не единственное, а тем более не главное средство

реагирования на вызов современности. В виду глобальности перемен, происходящих в государстве, бизнесе, самом образе жизни людей под воздействием цифровой революции, глобальная трансформация государственно-правовой системы неизбежна. Общегосударственный курс на цифровую трансформацию реализуется во всех государственных органах, в том числе прокуратуре¹.

К настоящему времени цифровая трансформация в отдельных правоохранительных органах привела к созданию таких электронных систем, как, например, «ГАС РФ Правосудие», ГИАЦ МВД России, АРМ следователя, государственная автоматизированная система «Правовая статистика» (ГАС ПС)², АИС «Адвокатура». Их можно считать прообразом будущей единой автоматизированной правоохранительной системы, агрегированной на цифровой платформе государства («государства-как-платформы») или цифровой уголовно-процессуальной экосистемы.

Контуров этой общей цифровой платформы взаимодействия правоохранительных органов угадываются в проекте Указа Президента Российской Федерации «О государственной автоматизированной системе правовой статистики»³. По мнению некоторых комментаторов, данная система имеет далеко идущее за рамки информационного обеспечения взаимодействие между прокуратурой и органами предварительного расследования в целях формирования единой базы статистических данных. Став управляющим субъектом государственной автоматизированной системы правовой статистики (ГАС ПС), Генеральная прокуратура России получает важное полномочие по управлению в целом системой органов предварительного расследования⁴.

Внедрение единой системы статистики для всех правоохранительных органов является, безусловно, необходимым и полезным делом. Мы разделяем мнение, что в организационно-управленческом плане полное введение в действие ГАС ПС повышает роль прокуратуры в

автоматизированной системе правовой статистики» (подготовлен Минюстом России 11.10.2016) // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PNPA&n=17452#017566841173639047> (дата обращения: 08.05.2021).

⁴ См.: Потапов Д. В. Проблемы взаимодействия следователя, руководителя следственного органа и прокурора в досудебном производстве по уголовному делу: дис. ... канд. юрид. наук. М.: Академия управления МВД России, 2019. С. 220.

¹ Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года: приказ Генпрокуратуры России от 14.09.2017 № 627 // Генеральная прокуратура РФ: официальный сайт [предшествующая версия]. URL: <https://genproc.gov.ru/documents/orders/627.pdf> (дата обращения: 08.05.2021).

² Портал технической поддержки ГАС ПС и дистанционного обучения. URL: <http://www.gasps-support.genproc.gov.ru> (дата обращения: 08.05.2021).

³ См.: пункт 4 Проекта Указа Президента Российской Федерации «О государственной

качестве управляющей подсистемы в системе правоохранительных органов. Это положительная тенденция. Хотя, надо подчеркнуть, это еще далеко от официального закрепления руководящей процессуальной роли прокуратуры в досудебном производстве и механизме выдвижения обвинения.

Вместе с тем, надо признать, что поэтапное внедрение системы государственной автоматизированной системы правовой статистики⁵ в деятельность ряда прокуратур и поднадзорных им органов на протяжении последних лет, проявило не только плюсы, но и минусы.

Нельзя не согласиться с мнением сотрудников органов внутренних дел, которое отражено в диссертационных исследованиях⁶ по поводу технических трудностей, возникших при внедрении этой системы на практике⁷, возрастания временных затрат, связанных с утверждением карточек статистической отчетности у надзирающего прокурора. Впрочем, опыт внедрения ГАС ПС позволяет говорить и о более серьезных

проявлениях известного феномена усиления бюрократических издержек под влиянием цифровых технологий.

Так, органы внутренних дел, испытывавшие применение системы ГАС СП, *вынуждены составлять статистическую отчетность дважды*: во-первых, в общей форме согласно ведомственным учетам правовой статистики предусмотренными совместным Приказом Генпрокуратуры России № 39 (МВД России № 1070) от 29.12.2005 «О едином учете преступлений»⁸, а, во-вторых, в системе ГАС ПС, которую требует прокуратура. При этом полностью отказываться от бумажных носителей статистической информации не желают ни в МВД, ни в прокуратуре. Получается, цифровизация по данному направлению (управления статистикой со стороны прокуратуры) привела к умножению работы сотрудников следственных органов и подразделений дознания МВД РФ.

Скептически оценивают представители научного сообщества и цифровую систему учета материалов проверок и уголовных дел (УМПИУД).

⁵ О государственной автоматизированной системе правовой статистики прокуратуры Российской Федерации // Генеральная прокуратура РФ: официальный сайт [предшествующая версия]. URL: <https://genproc.gov.ru/smi/news/regionalnews/news-1042623/> (дата обращения: 08.05.2021).

⁶ См., напр.: Кудряшова Е. С. Обеспечение качества дознания в уголовном судопроизводстве: дис. ... канд. юрид. наук. Н. Новгород, 2020. С. 116–118, 127 и след.

⁷ На момент возбуждения уголовного дела, сотруднику, ведущему расследование по уголовному делу в форме дознания или следствия, необходимо предоставить прокурору: сопроводительное письмо в 2-х

экземплярах, копию постановления о возбуждении уголовного дела, надзорный материал, статистические карточки на возбужденное уголовное дело.

⁸ Инструкция о порядке заполнения и предоставления учетных документов (Приказ Генпрокуратуры России № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 (ред. от 20.02.2014) «О едином учете преступлений» (Зарегистрировано в Минюсте России 30.12.2005 № 7339) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2006. № 5. С. 3–19.

Официально целью работы данной системы является учет зарегистрированных органами внутренних дел в КУСП⁹ материалов проверок, осуществляемых в порядке статей 144–145 УПК РФ и возбужденных уголовных дел. Так, сотрудник дежурной части вносит в систему УМПИУД данные по каждому материалу проверки с присвоением номера в соответствии с номером зарегистрированного в КУСП сообщения и краткие сведения о произошедшем. В последующем к зарегистрированному в системе УМПИУД материалу прикрепляется электронная копия принятого решения как со стороны ОВД (постановление об отказе в возбуждении уголовного дела), так и органов прокуратуры (постановление об отмене постановления об отказе в возбуждении уголовного дела). По уголовным делам, лицо, осуществляющее расследование, вносит в систему УМПИУД сведения по возбужденному уголовному делу – номер, дату, квалификацию преступления, сведения о лице, совершившем преступление, предмет преступного посягательства, сумму материального ущерба, сведения о

лице, осуществляющем расследование, а также данные о наличии надзора со стороны надзирающих органов. В систему учета вносятся сведения о движении уголовного дела – продление срока расследования, а также результаты расследования уголовного дела с прикреплением утвержденной прокурором электронной копии принятого процессуального решения, завершающего досудебное производство¹⁰. Все это ложится дополнительной нагрузкой на сотрудников органов предварительного следствия и дознания.

Таким образом, сотрудники органов внутренних дел вынуждены ввести два производства: одно в письменном виде, а его копию – в электронном (для надзирающего органа). Это тот негативный вариант цифровой трансформации уголовно-процессуальной системы¹¹, которого желательно было бы избежать. Но пока реальность именно такова: вместо повышения эффективности деятельности правоохранителей она ведет к увеличению внутрисистемных и не нужных обществу затрат.

⁹ Книга учета заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях в соответствии с Приказом МВД России от 29 августа 2014 г. № 736 (ред. от 09.10.2019) «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях» (Зарегистрировано в Минюсте России 06.11.2014 № 34570) // СПС «КонсультантПлюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_170872/9ce7287a3d69066c98df57e6f4ba5d953127bd02/ (дата обращения: 08.05.2021).

¹⁰ См.: Кудряшова Е. С. Обеспечение качества дознания в уголовном судопроизводстве: дис. ... канд. юрид. наук. Н. Новгород, 2020. С. 201.

¹¹ См.: Потапов Д. В. Проблемы взаимодействия следователя, руководителя следственного органа и прокурора в досудебном производстве по уголовному делу: дис. ... канд. юрид. наук. М.: Академия управления МВД России, 2019. С. 200–201.

Нельзя не согласиться с тем, что имевшие место попытки внедрения цифровых технологий в практику предварительного расследования, прокурорского надзора за процессуальной деятельностью органов следствия и дознания привели вместо повышения ее эффективности к умножению бюрократической сущности правоохранительной системы¹².

Поэтому вместо того, чтобы продолжать цифровую трансформацию в прежнем духе, следовало бы задаться вопросом о том, подлежит ли оцифровке в принципе существующая — следственная — уголовно-процессуальная модель.

Как известно по данному вопросу преобладает положительный ответ со стороны большинства отечественных процессуалистов. Наиболее развита эта позиция в работах С. В. Зуева, который высказывается за создание единой автоматизированной экосистемы

уголовного судопроизводства (ЕАЭ УСП)¹³.

Прообразом такой системы может служить «Электронное уголовное дело»¹⁴. При этом следует учитывать опыт зарубежных государств в проведении цифровой трансформации своих правовых систем противодействия преступности, в том числе и казахстанский опыт, который весьма поучителен¹⁵.

Но прежде обозначим альтернативную точку зрения относительно перспективы цифровой трансформации отечественного уголовного судопроизводства. По мнению ряда исследователей, технократический подход недостаточен для решения проблемы трансформации правовой системы противодействия преступности в условиях цифровизации. Внедрение цифровых технологий должно сопровождаться реформированием уголовно-процессуального механизма¹⁶.

¹² См.: Власова С. В. Теоретическая концепция правовой (уголовно-процессуальной) организации противодействия преступности в сфере экономики: монография. М.: Юрлитинформ, 2020. С. 346–350.

¹³ Зуев С. В. Стратегия развития уголовного судопроизводства в условиях цифровизации: авторская концепция. // Международная Ассоциация Содействия Правосудию. URL: <https://www.iauaj.net/node/2833> (дата обращения: 08.05.2021); Информационные технологии в уголовном процессе зарубежных стран: монография / под ред. докт. юрид. наук С. В. Зуева. М.: Юрлитинформ, 2020. С. 172–180.

¹⁴ См., напр.: Качалова О. В., Цветков Ю. А. Электронное уголовное дело — инструмент модернизации уголовного судопроизводства

// Российское правосудие. 2015. № 2. С. 95–101; Адамович О. А. Электронное уголовное дело: перспективы и проблемы внедрения // Теоретико-прикладные вопросы развития досудебного производства по уголовным делам на современном этапе: сб. ст. междунар. науч.-практ. конф., Новополюцк, 26–27 сент. 2019 г.: в 2 т. / Полоц. гос. ун-т; редкол.: И. В. Вегера (отв. ред) [и др.]. Новополюцк, 2019. Т. 2. С. 5–17.

¹⁵ См., напр.: Зуев С. В. Цифровая среда уголовного судопроизводства: проблемы и перспективы // Сибирский юридический вестник. 2018. № 4. С. 118–123.

¹⁶ См.: Власова С. В. Теоретическая концепция правовой (уголовно-процессуальной) организации противодействия преступности в сфере

Мы поддерживаем идею, согласно которой цифровая революция позволяет перейти от следственного к состязательному виду уголовного судопроизводства, а равно – от следственной и односторонней уголовно-процессуальной модели доказывания к состязательной, открытой, судебной модели доказывания основания решения о применении уголовного закона. Только реформированная состязательная модель уголовного судопроизводства должна быть агрегирована на цифровой платформе государства. При этом прокуратуре должны быть предоставлены решающие полномочия по проведению досудебного уголовного расследования и выдвижению обвинения¹⁷.

Сторонниками смены уголовно-процессуальной модели при ее цифровой трансформации предлагается поменять технологию доказывания по схеме «агент уголовного розыска («следователь») – прокурор – судебный орган»¹⁸. Информационное взаимодействие между прокурором и агентом обвинительной власти («следователем») должно, согласно данному подходу, происходить вокруг формирования «обвинительных доказательств», то есть тех

фактических материалов, представленных в любом виде, по любым каналам связи, на любых носителях информации (в том числе, электронных носителях), которые могут быть представлены прокурором суду в обоснование обвинения¹⁹.

В этом состоит суть трансформации уголовно-процессуальной системы: вначале ее реформа по состязательной модели, отказ от письменного, следственного порядка выдвижения обвинения и формирования уголовно-процессуальных доказательств, а затем перенос этой системы на цифровую платформу.

Опыт Казахстана в этом плане поучителен, поскольку показывает именно подобную последовательность: вначале реформа предварительного расследования, затем цифровая трансформация уголовно-процессуальной системы. Казахстан существенно реформировал свое досудебное производство, приняв в 2014 году новый уголовно-процессуальный кодекс. Хотя следственная модель доказывания в принципиальных чертах была сохранена. В 2017 году в Уголовно-процессуальный кодекс Республики Казахстан внесены изменения в виде статьи 42-1, предусматривающие

экономики: монография. М.: Юрлитинформ, 2020. С. 361.

¹⁷ См., напр.: Александров А. С., Андреева О. И., Зайцев О. А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации // Вестн. Том. гос. ун-та. 2019. № 448. С. 199–207.

¹⁸ См.: Потапов Д. В. Проблемы взаимодействия следователя, руководителя следственного органа и прокурора в

досудебном производстве по уголовному делу: дис. ... канд. юрид. наук. М.: Академия управления МВД России, 2019. С. 211–213.

¹⁹ См. Потапов Д. В. Проблемы взаимодействия следователя, руководителя следственного органа и прокурора в досудебном производстве по уголовному делу: дис. ... канд. юрид. наук. М.: Академия управления МВД России, 2019. С. 219–220.

«электронный формат уголовного судопроизводства».

В 2021 году было принято политическое решение о проведении более радикальной реформы досудебного производства и модели уголовно-процессуального доказывания. В Послании Главы государства Касым-Жомарта Токаева народу Казахстана от 1 сентября 2020 г. «Казахстан в новой реальности: время действий» было указано на необходимость модернизации уголовной сферы по примеру развитых стран ОЭСР с внедрением трехзвенной модели с четким разделением полномочий между органами уголовного преследования, прокуратурой и судом на стадии досудебного расследования²⁰.

В развитие идеи о трехзвенной уголовной модели была разработана Концепция к проекту Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам внедрения трехзвенной модели с разграничением полномочий и зон ответственности между правоохранительными органами, прокуратурой и судом»²¹.

Согласно этой концепции три

ключевые задачи уголовного процесса будут выполняться разными органами:

1) выявление, пресечение преступления, установление причастных лиц, сбор и закрепление доказательств – органами досудебного расследования;

2) дача независимой оценки собранным доказательствам, принятие ключевых процессуальных решений, предъявление и поддержание обвинения в суде – прокуратурой;

3) назначение наказания, рассмотрение жалоб граждан – судом.

При этом на прокурора будут возложены ключевые процессуальные функции, определяющие ход предварительного расследования и переход дела в судебную стадию. Законодательное возложение на прокурора обязанности по согласованию процессуальных решений по уголовным делам, совмещенное с цифровизацией уголовного процесса, представляет собой эффективную площадку для дальнейшего разграничения полномочий и зон ответственности между органами уголовного преследования²².

²⁰ Послание Главы государства Касым-Жомарта Токаева народу Казахстана. 1 сентября 2020 г. // Официальный сайт Президента Республики Казахстан. URL: https://www.akorda.kz/ru/addresses/addresses_of_president/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-1-sentyabrya-2020-g (дата обращения: 08.05.2021).

²¹ Концепция к проекту Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам внедрения трехзвенной модели с

разграничением полномочий и зон ответственности между правоохранительными органами, прокуратурой и судом» // Генеральная Прокуратура Республики Казахстан: официальный сайт. URL: [ghttps://www.gov.kz/memleket/entities/prokuror/press/news/details/186080?lang=kk](https://www.gov.kz/memleket/entities/prokuror/press/news/details/186080?lang=kk) (дата обращения: 08.05.2021).

²² См. Концепция к проекту Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам внедрения

Таким образом, казахстанский опыт вполне убедительно доказывает, что без реформы предварительного расследования, которую провели почти все постсоветские государства, цифровая трансформация уголовно-процессуальной системы

бесперспективна, более того она чревата рисками для прав и свобод человека и гражданина. Проект «электронное уголовное дело», предполагающий трансформацию следственной модели в цифровую среду, бесперспективен.

Список литературы

1. Адамович О. А. Электронное уголовное дело: перспективы и проблемы внедрения // Теоретико-прикладные вопросы развития досудебного производства по уголовным делам на современном этапе: сб. ст. междунар. науч.-практ. конф., Новополоцк, 26–27 сент. 2019 г.: в 2 т. / Полоц. гос. ун-т; редкол.: И. В. Вегера (отв. ред.) [и др.]. Новополоцк, 2019. Т. 2. С. 5–17.

2. Александров А. С. О перспективах развития российского уголовного судопроизводства в условиях цифровизации / А. С. Александров, О. И. Андреева, О. А. Зайцев // Вестник Томского государственного университета. 2019. № 448. С. 199–207.

3. Власова С. В. Теоретическая концепция правовой (уголовно-процессуальной) организации противодействия преступности в сфере экономики: монография. М.: Юрлитинформ, 2020. 440 с.

4. Зуев С. В. Стратегия развития уголовного судопроизводства в условиях цифровизации: авторская концепция // Международная Ассоциация Содействия Правосудию. URL: <https://www.iuaj.net/node/2833>.

5. Зуев С. В. Цифровая среда уголовного судопроизводства: проблемы и перспективы // Сибирский юридический вестник. 2018. № 4. С. 118–123.

6. Информационные технологии в уголовном процессе зарубежных стран: монография / под ред. докт. юрид. наук С. В. Зуева. М.: Юрлитинформ, 2020. 216 с.

7. Качалова О. В. Электронное уголовное дело – инструмент модернизации уголовного судопроизводства / О. В. Качалова, Ю. А. Цветков // Российское правосудие. 2015. № 2. С. 95–101.

8. Кудряшова Е. С. Обеспечение качества дознания в уголовном судопроизводстве: дис. ... канд. юрид. наук. Н. Новгород, 2020. 262 с.

9. Потапов Д. В. Проблемы взаимодействия следователя, руководителя следственного органа и прокурора в досудебном производстве по уголовному делу: дис. ... канд. юрид. наук. М.: Академия управления МВД России, 2019. 206 с.

трехзвенной модели с разграничением полномочий и зон ответственности между правоохранительными органами, прокуратурой и судом» // Генеральная Прокуратура Республики Казахстан:

официальный сайт. URL: <https://www.gov.kz/memleket/entities/prokuror/press/news/details/186080?lang=kk> (дата обращения: 08.05.2021).

Oleg V. Levchenko

PhD (Law),

Prosecutor of Troitsky and Novomoskovsky

administrative districts of Moscow

(Moscow, Russian Federation)

2923757@rambler.ru

**PROCEDURAL AND LEGAL FORM OF INTERACTION
OF THE PROSECUTOR'S OFFICE AND THE PRELIMINARY
INVESTIGATION BODIES IN THE ACTION OF CRIME IN THE
CONDITIONS OF DIGITALIZATION**

Abstract: The digital transformation of the criminal procedural system should take place after the reform of the preliminary investigation and the transition to an adversarial type of criminal proceedings. In the new criminal procedure model, installed on the digital platform of the state, the prosecutor should take a leading role in relation to the preliminary investigation bodies, authorized to detect, solve and investigate crimes, and decide on the referral of the case to the court.

Keywords: prosecutor, preliminary investigation bodies, criminal procedure, digital transformation.

УДК 343.98

Бердникова Ольга Петровна

Кандидат юридических наук, доцент кафедры криминалистики,

Уральский юридический институт МВД России

(г. Екатеринбург, Российская Федерация)

berdnikovs@inbox.ru

Блинова Ксения Николаевна

Курсант,

Уральский юридический институт МВД России

(г. Екатеринбург, Российская Федерация)

berdnikovs@inbox.ru

НЕКОТОРЫЕ ОСОБЕННОСТИ ЛИЧНОСТИ МОШЕННИКА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация: В статье раскрываются криминалистические особенности, раскрывающие личность преступника, совершающего мошеннические действия в сфере компьютерной информации. Отмечены возрастные критерии преступников в сфере компьютерной информации, которые разделить на две группы: первую группу составляют лица примерно 16–22 лет; вторую группу составляют лица старше 23 лет.

Ключевые слова: мошенничество, IT-технологии, компьютерная информация, личность преступника.

Для цитирования:

Бердникова О. П. Некоторые особенности личности мошенника в сфере компьютерной информации / О. П. Бердникова, К. Н. Блинова // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 345–349.

Нельзя не заметить, что на сегодняшний день происходит стремительное развитие и повсеместное внедрение в жизнь человека компьютерных технологий. Это обуславливается большим количеством факторов, так как с каждым последующим годом «искусственный интеллект» используется не только профессионалами, но и обывателями в повседневной деятельности. Теперь

процедура по получению доступа в сеть Интернет не является затруднительной, поскольку практически у каждого имеется мобильный телефон, который позволяет без проблем оперативно и в любом объеме найти необходимую информацию.

Однако, как показывает практика, люди стали применять цифровые новшества не только для упрощения жизни и быстрого решения

задач, но и для реализации своих корыстных целей, например, таких, как завладение чужими деньгами посредством обмана, получение доступа к чужим данным различными путями и так далее.

В подтверждение актуальности темы следует также отметить ежегодный рост преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Только за 2020 год их количество возросло на 73,4 %. При этом совершение таких преступлений с использованием сети Интернет выросло на 91,3 %, посредством мобильной связи – на 88,3 %. Общее число мошенничеств в сфере компьютерной информации выросло на 10,8 %¹. К сожалению, тенденции роста не снижаются. Так, за январь–март 2021 года количество указанных преступлений выросло на 49,6 %, совершенных с использованием сети Интернет – на 51,6 %, сотовой связи – на 31,6 %. Число мошенничеств в сфере компьютерной информации выросло в отчетном периоде на 16,9 %².

Немаловажным аспектом является звено системы криминалистической характеристики преступления, которое отражает личность лица, совершившего противоправное деяние. Стоит учитывать некоторые особенности

рассматриваемого компонента, потому как это позволит правоохранительным органам определить круг подозреваемых и структурировать свои действия в определенном порядке, и если пользователи гаджетов и электронно-вычислительных машин будут обращать внимание на данные характерные свойства, присущие IT-мошенникам, то, возможно, заявлений от пострадавших в области мошенничества в сфере компьютерной информации станет немного меньше.

К особенностям личности киберпреступника можно отнести следующее:

- безупречное знание устройства того средства, которое используется для претворения в жизнь противоправного умысла;
- однозначно выражает задачи, но в то же время обладает бессистемным поведением в повседневности;
- в преступной деятельности все свои действия выстраивает логически, последовательно, но в обыденной жизни мышление зачастую подводит;
- имеет небольшой круг общения, отдавая предпочтение тем людям, которые так же, как и он, увлекаются информационными технологиями;

¹ Состояние преступности в России за январь–декабрь 2020 года: сборник статистики и аналитики МВД России // Министерство внутренних дел РФ: официальный сайт. URL: <https://мвд.рф/reports/item/22678184/> (дата обращения: 13.05.2021).

² Состояние преступности в России за январь–март 2021 года сборник статистики и аналитики МВД России // Министерство внутренних дел РФ: официальный сайт. URL: <https://мвд.рф/files/application/2111940> (дата обращения: 13.05.2021).

- предрасположенность к творческому подходу при выстраивании противоправных тактик, способных внушить убежденность у людей в наличии благих намерений;

- речь довольно-таки предметна, ориентирована, конкретна, имеется такое своеобразие как привычка часто переспрашивать, делать ненужный акцент на каких-либо деталях, не имеющих важного значения, тем самым вызывает у оппонента негодование;

- чрезмерное применение в беседе слов, употребляемых людьми, работающих с компьютерами, для того, чтобы потянуть время допроса, запутать должностное лицо, пустить его по ложному следу, дать понять представителю органа государственной власти, что он не сможет быть с подозреваемым «на одной волне» и что ему придется предпринять дополнительные меры для получения значимой информации.

Сетевых злоумышленников, промышляющих мошенничеством в сфере компьютерной информации, бесчисленное множество. Кто-то из них имеет соответствующее образование, а кто-то приобретает умения и навыки непосредственно при работе с устройствами и поисковыми системами. Учитывая это, условно преступное звено можно поделить на две группы. К первой следует отнести лиц, которые находились в какой-либо связи с потерпевшим, например, к такой ситуации будет относиться следующая: работник службы безопасности юридической компании удаляет важные данные, используемые в трудовой

деятельности, с ПК своего напарника. Во вторую же группу входят лица, не состоящие с потерпевшим ни в каких отношениях. Важно отметить, что в большей степени мошенники посредством Всемирной сети совершают свои противоправные деяния с прямым умыслом.

Важно отметить, что по возрастному критерию преступников в сфере компьютерной информации следует разделить на две группы.

Первую группу составляют лица примерно 16–22 лет. Это школьники старших классов или студенты, обучающиеся в средне-специальных учебных заведениях с техническим уклоном, а чаще лица, обучающиеся в высших учебных заведениях по специальностям, связанным с информационными технологиями. Данные лица обычно совершают преступление впервые; предметом преступления чаще всего являются незначительные денежные суммы. О совершении мошенничества указанной категорией лиц также свидетельствует отсутствие тщательной подготовки и сокрытия преступления.

Вторая группа – лица старше 23 лет. Эти лица уже получили высшее образование и имеют определенные специальные знания в сфере компьютерных технологий, у них есть опыт совершения определенных преступных воздействий с помощью вмешательств в функционирование средств хранения, обработки или передачи компьютерной информации. Они отличаются осознанностью, обладают определенным профессионализмом. Преступные действия носят многоэпизодный

характер с наличием круга потерпевших, причинением значительного материального ущерба, характеризуются тщательной подготовкой к совершению и сокрытию следов преступления. На долю данной группы приходится большинство общественно опасных преступлений, совершаемых с использованием средств компьютерной техники, присвоений денежных средств в особо крупных размерах, мошенничества и пр.³

Как правило, работники, находящиеся на руководящих должностях, обладают широкопрофильным уровнем знаний, позволяющих иметь в своем распоряжении объем конфиденциальной информации, в связи с чем им легче материализовать свои криминальные цели. Принимая это во внимание, можно указать еще одну классификацию коммуникационных злоумышленников. В первую группу будут входить лица, искусно обладающие программированием, проявляющие непомерный интерес ко

всему, что связано с доступом ко Всемирной паутине, вторую группу будут составлять лица, страдающие психическими заболеваниями, которые не дают человеку воспринимать действительной таковой, какой она является на самом деле, вследствие чего снижается способность принимать благоразумное решение, к третьей группе относятся те, кто используют информационную сеть «Интернет» для реализации своих меркантильных мотивов, они-то и представляют наибольшую опасность для общества и государства в целом⁴.

Обобщая вышесказанное, хочется сказать, что органам и должностным лицам, борющимся с мошенничеством в сфере компьютерной информации, необходимо исследовать личности преступников и выделять их исключительные черты, так как это может поспособствовать успешному обнаружению лиц и в целом благополучному расследованию преступления.

Список литературы

1. Криминалистика: углубленный курс / под ред. А. Г. Филипова. М.: ДГСК МВД России, 2012.
2. Протасевич А. А. Криминалистическая характеристика компьютерных преступлений / А. А. Протасевич, Л. П. Зверьянская // Российский следователь. 2013. № 11. С. 45–47.

³ См.: Криминалистика: углубленный курс / под ред. А. Г. Филипова. М.: ДГСК МВД России, 2012. С. 136.

⁴ Протасевич А. А., Зверьянская Л. П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. № 11. С. 45–47.

Olga P. Berdnikova

PhD (Law), Associate Professor of the Department of Criminalistics,
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
berdnikovs@inbox.ru

Ksenia N. Blinova

Cadet,
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
berdnikovs@inbox.ru

SOME FEATURES OF THE IDENTITY OF A FRAUDSTER IN THE FIELD OF COMPUTER INFORMATION

Abstract: The article reveals the criminalistic features that reveal the identity of the criminal who commits fraudulent actions in the field of computer information. The age criteria of criminals in the field of computer information are noted, which are divided into two groups: the first group consists of persons approximately 16-22 years old; the second group consists of persons over 23 years old.

Keywords: fraud, IT-technologies, computer information, the identity of the criminal.

Гаскаров Ильдус Фанавиевич

Кандидат юридических наук, доцент, доцент кафедры криминалистики,
Уральский государственный юридический университет
(г. Екатеринбург, Российская Федерация)
madagaskar.15@mail.ru

Ефимов Данил Сергеевич

Студент,
Уральский государственный юридический университет
(г. Екатеринбург, Российская Федерация)
danilefimov00@mail.ru

**ОСОБЕННОСТИ ВЫЯВЛЕНИЯ И ДОКУМЕНТИРОВАНИЯ ФАКТОВ
ВЗЯТОЧНИЧЕСТВА ПРИ ОСУЩЕСТВЛЕНИИ ОПЕРАТИВНО-
РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

Аннотация: В представленной статье рассматриваются особенности выявления и документирования фактов взяточничества. Особое внимание уделяется проблемам правоприменения в рамках осуществления оперативно-розыскной деятельности. Так, в статье исследуются поисковые признаки, указывающие на возможность подготовки и совершения взяточничества, рассматриваются оперативно-розыскные мероприятия, позволяющие получить оперативно-значимую информацию и задокументировать факты взяточничества, в том числе с использованием информационных технологий.

Ключевые слова: взяточничество, оперативно-розыскная деятельность, оперативный поиск, оперативно-розыскные мероприятия, опрос, оперативный эксперимент, информационные технологии.

Для цитирования:

Гаскаров И. Ф. Особенности выявления и документирования фактов взяточничества при осуществлении оперативно-розыскной деятельности с использованием информационных технологий / И. Ф. Гаскаров, Д. С. Ефимов // Технологии XXI века в юриспруденции: материалы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 350–360.

Одним из видов преступлений, требующим постоянного и пристального внимания правоохранительных органов, безусловно, является взяточничество. Опасность этого преступления

заключается в дискредитации государственной власти, её представителей, повышении уровня коррупции в органах власти и стране в целом, а также усилении пренебрежения к закону. Вопрос

взяточничества в современной России является наиболее острым, ведь преступления такого рода подрывают основы государственной деятельности и управления, затрагивают права и законные интересы граждан. При этом нельзя говорить о том, что проблема коррупции, в частности, взяточничества, только проблема сегодняшнего дня. Вполне допустимо говорить о том, что она возникла вместе с образованием государства.

Данной проблемой в разное время занимались такие исследователи как Р. С. Белкин, Л. Я. Драпкин, В. Н. Карагодин, Кушниренко С.П. и другие¹. Также данный вопрос рассматривался в диссертациях Е. В. Христиной, А. Н. Марданова². Стоит также заметить, что актуальность данной темы поднимается не только в науке, но также и в культуре. В качестве такого примера можно привести фильм «Белое солнце пустыни», в котором Верещагин, роль которого исполнил П. Б. Луспекаев, реагируя на предложение ещё одного героя фильма Абдуллы о взятке произносит фразу, ставшую крылатой: «Я мзду не беру – мне за Державу обидно!». Сам же герой стал символом неподкупности.

Выявление и раскрытие взяточничества практически не обходится без участия оперативно-розыскных служб и их возможностей,

поскольку данному виду преступления присущ латентный характер, объясняемый желанием субъектов, участвующих в этом противоправном проявлении, скрывать свои преступные действия и намерения. Именно в связи с этим о значительной части совершаемых преступлений данного вида в большинстве случаев становится известно в результате осуществления комплекса оперативно-розыскных мероприятий.

Своевременное поступление информации о противоправной деятельности, поиск и обнаружение дополнительных сведений, надлежащая проверка полученных данных, позволяют должностным лицам оперативных подразделений правильно оценивать складывающуюся ситуацию и определять не только направления осуществления оперативно-розыскной деятельности, но и возможности реализации полученной, проверенной и задокументированной информации в рамках уголовного судопроизводства.

Одним из основных методов поступления информации о подготавливаемом, совершаемом или совершенном взяточничестве является поиск сотрудниками оперативных подразделений первичных сведений, указывающих на возможную подготовку или совершение

преступлений: учебное пособие. 2-е изд. Екатеринбург, 2013.

² Христинина Е. В. Особенности расследования получения взятки в системе высшего образования // диссертация на соискание ученой степени кандидата юридических наук, 2016.

¹ Криминалистика в 3 ч. Часть 1 : учебник для вузов / Л. Я. Драпкин [и др.]; ответственный редактор Л. Я. Драпкин. 2-е изд., испр. и доп. Москва: Издательство Юрайт, 2019. 246 с. Режим доступа: ЭБС Юрайт [сайт]. URL: <https://urait.ru/bcode/434587> (дата обращения: 15.05.2021).; Карагодин В. Н., Вахмянина Н. Б. Методика расследования должностных

преступления на конкретном объекте оперативного обслуживания либо возможную подготовку или совершение взяточничества конкретным лицом. Очевидно, что в основе направленности поисковых действий, осуществляемых оперативными сотрудниками, будут лежать факторы, обнаружение которых может косвенно указывать на возможность подготовки и совершения преступления рассматриваемого вида.

К их числу мы отнесли личностно-поведенческие (характеризующие должностное лицо и его доступность в решении служебных вопросов, определяющие возможности организации и проведения досуга, а также характер его связей); корпоративные (сложившиеся устои осуществления деятельности в организации или учреждении); имущественные (определяющие благосостояние лица и возможность иметь соответствующее имущество); документальные (свидетельствующие о проведении различных операций и движении материальных, технических средств, объектов недвижимости); сведения поступившие от граждан (коллеги, взяткодатели и иные лица; а также обнаружение очевидных следов преступной деятельности – предметы взятки или оказанные услуги и т. п.).

К числу оперативно-розыскных мероприятий, осуществляемых на стадии оперативного поиска, следует отнести: опрос (осуществляемый в связи с предполагаемой позицией объекта опроса в различных формах), наведение справок, обследование служебных помещений, сбор образцов

для сравнительного исследования, исследование предметов и документов, наблюдение.

В части решения задач по выявлению взяточничества на участке или объекте обслуживания, наряду с изучением оперативной обстановки, осуществлением оперативного поиска, оперативные сотрудники используют предоставленное им право устанавливать на безвозмездной либо возмездной основе отношения сотрудничества с лицами, изъявившими согласие оказывать содействие на конфиденциальной основе органам, осуществляющим оперативно-розыскную деятельность (см. ст. 15 ФЗ «Об оперативно-розыскной деятельности»).

Проведение аналитической работы, по результатам проведённых поисковых оперативно-розыскных мероприятий позволяет выдвигать соответствующие версии о возможной противоправной деятельности и приступать к более детальной их проверке. При наличии данных указывающих на подготовку или причастность к совершению взяточничества конкретных лиц, оперативные сотрудники в первую очередь обращаются к информационным системам и проверяют данных лиц по оперативно-справочным и криминалистическим учетам, которые позволяют получить сведения о возможном привлечении или освобождении от уголовной ответственности, наличии материалов проверки в отношении данных лиц, по которым было принято решение об отказе в возбуждении уголовного

дела, наличии других компрометирующих данных³.

Информационные технологии, являющиеся практически неотъемлемой частью жизни большинства людей, позволяют лицам создавать профили в социальных сетях и сохранять там различные сведения. В связи с этим, оперативным сотрудникам, осуществляющим проверку лиц по факту готовящегося или совершённого взяточничества, целесообразно осмотреть профили проверяемых лиц в социальных сетях, изучить их связи и копировать необходимые для решения задач сведения⁴.

В рамках оперативного изучения проверяемого лица, безусловно, обращается внимание на исследование аспектов деятельности данного лица, связанных с исполнением им профессиональных обязанностей. В этой связи изучаются документы административно-хозяйственной деятельности лица. Безусловно, некоторая часть информации, касающаяся совершения взяточничества, может поступить от лиц, оказывающих содействие органам, осуществляющим оперативно-розыскную деятельность

(ст. 17 ФЗ «Об оперативно-розыскной деятельности»).

Самым оптимальным развитием оперативно-розыскной ситуации, складывающейся при осуществлении проверки информации о взяточничестве, является получение данных о предполагаемом взяткодателе. Тщательное изучение личности взяткодателя должно позволить оперативным сотрудникам определить возможные способы установления с ним необходимого контакта и проведения работы, направленной на оказание помощи оперативным сотрудникам в выявлении взяткополучателя и документировании осуществляемых последним преступных действий. Практика показывает, что в большинстве случаев основным средством убеждения необходимости оказать содействие органам, осуществляющим оперативно-розыскную деятельность, является освобождение от уголовной ответственности в соответствии с примечанием к ст. 291 УК РФ⁵.

Если совокупность сведений, указывающих на противоправный характер деятельности устанавливаемого лица-взятополучателя, является

³ Начальная профессиональная подготовка и введение в специальность: правоохранительная деятельность : учебник для среднего профессионального образования / Д. В. Бахтеев, И. Ф. Гаскаров [и др.]; ответственный редактор Д. В. Бахтеев. М.: Издательство Юрайт, 2019. Режим доступа: ЭБС Юрайт [сайт]. URL: <https://urait.ru/bcode/442093> (дата обращения: 13.05.2021). С. 230–231.

⁴ Правовые основы проведения оперативно-розыскных мероприятий в целях выявления

и документирования получения взяток : учебно-методическое пособие / М. Л. Родичев [и др.]. СПб.: ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации», 2018. С. 21.

⁵ Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 14.05.2021).

достаточной, то в соответствии со ст. 10 ФЗ «Об оперативно-розыскной деятельности» органы, осуществляющие оперативно-розыскную деятельность, заводят дело оперативного учёта для документирования преступной деятельности. Несмотря на то, что факт заведения дела оперативного учёта не является основанием для ограничения конституционных прав граждан, именно в рамках дела оперативного учёта осуществляется большинство оперативно-розыскных мероприятий, позволяющих, в том числе, получать оперативным сотрудникам информацию с применением информационных технологий.

Первоочередным оперативно-розыскным мероприятием будет являться опрос предполагаемого взяткодателя, надлежащая организация и проведение которого позволит установить факты и обстоятельства, известные опрашиваемому лицу и способствующие принятию оперативными сотрудниками верных тактических решений по проведению комплекса оперативно-розыскных мероприятий в целях решения задач по выявлению, пресечению и раскрытию конкретного факта взяточничества. При этом целесообразно принять меры, которые будут способствовать снижению

риска утечки информации, а также создать условия, которые predispose взяткодателя к дальнейшему сотрудничеству⁶.

При опросе взяткодателя следует произвести видеофиксацию, поскольку она в полной мере позволяет подтвердить законность действий сотрудников, а также зафиксировать необходимые показания, которые позволят проводить дальнейшие оперативно-розыскные мероприятия.

Проводя опрос, оперативным сотрудникам следует достоверно установить факт требования передачи взятки, способ осуществления требования о передаче (аудиальный или с помощью электронной переписки в мессенджерах), определить предмет взятки, способ его передачи, который может быть, в том числе, и бесконтактным и т. п.

В случае предполагаемого бесконтактного способа оплаты, например, путём перевода денежных средств, необходимо обращаться в суд, так как в соответствии с частью 5 статьи 26 ФЗ «О банках и банковской деятельности» справки по операциям, счетам и вкладам физических лиц выдаются на основании судебного решения кредитной организацией должностным лицам органов, уполномоченных осуществлять оперативно-розыскную деятельность, при выполнении ими функций по

⁶ Правовые основы проведения оперативно-розыскных мероприятий в целях выявления и документирования получения взяток : учебно-методическое пособие / М. Л. Родичев [и др.]. СПб.: ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации», 2018. С. 19.

выявлению, предупреждению и пресечению преступлений по их запросам, направляемым в суд в порядке, предусмотренном статьей 9 ФЗ «Об оперативно-розыскной деятельности», при наличии сведений о признаках подготавливаемых, совершаемых или совершённых преступлений, а также о лицах, их подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела.

Важной задачей проведения опроса является также исключение факта провокации самим взяточдателем. При этом выясняются возможные последствия для взяточдателя в случае, если взятка не будет передана. В этом случае, сотруднику оперативного подразделения необходимо определить оптимальные пути содействия взяточдателю в решении данной проблемы, что также расположит его к сотрудничеству.

При установлении в ходе опроса факта переписки взяточдателя с взяточполучателем, необходимо установить какой мессенджер конкретно используется (WhatsApp, Viber, Telegram)⁷. В этом случае оперативными сотрудниками проводится оперативно-розыскное мероприятие – снятие информации с технических каналов связи. В комплексе, при необходимости могут

быть проведены и другие оперативно-розыскные мероприятия, связанные с использованием современных информационных технологий (прослушивание телефонных переговоров, получение компьютерной информации).

При этом необходимо иметь в виду следующие особенности проведения данных мероприятий:

- данные мероприятия осуществляются на основании судебного решения, поскольку связаны с ограничением конституционных прав человека и гражданина (ст. 8 ФЗ «Об оперативно-розыскной деятельности»);

- являются негласными мероприятиями, имеющими направленность на получение тщательно скрываемой информации, способствующей раскрытию преступления и изобличению лица, его совершающего или совершившего⁸;

- требуют использования специальных технических и информационных средств, технологий, специально разработанного программного обеспечения, с помощью которых осуществляются данные мероприятия.

Результаты проведенных соответствующих мероприятий отражаются в составляемых оперативными сотрудниками документах (рапорт или справка), к которым прилагаются

⁷ Коломиец А. В., Ибляминова Э. Р. К вопросу о методике расследования современных способов совершения взятничества с использованием мессенджеров // Научный электронный журнал «Меридиан». 2020. № 4 (38).

⁸ Павличенко Н. В., Самоделкин А. С. Негласность в оперативно-розыскной деятельности // Вестник Волгоградской академии МВД России. 2012. № 3 (22).

соответствующие носители (помещенные в упаковку и опечатанные) с полученной информацией⁹. Хранятся носители данной информации в условиях, исключающих к ним доступ третьих лиц. Представление полученных материалов органу расследования осуществляется только в случае возможности соблюдения требований конспирации, в остальных случаях данная информация используется в рамках дел оперативного учёта, для решения задач оперативно-розыскной деятельности.

Завершающим оперативно-розыскным мероприятием по документированию факта взятничества и приближающим оперативных сотрудников к реализации собранных материалов является оперативный эксперимент, позволяющий задержать преступника с поличным.

Для успешного проведения «оперативного эксперимента», а также исключения возможных препятствий в виде провокации взятки, до задержания взяткополучателя с поличным, желательно, по возможности, провести встречу между взяткодателем и взяткополучателем, в ходе которой будет производиться аудио- или видеофиксация. При встрече взяткодателю в ненавязчивой форме следует выяснить такие вопросы как: размер взятки, способ, место и время её передачи.

Чтобы исключить факт провокации взятки, оперативному сотруднику следует обговорить с взяткодателем все детали предстоящей встречи, объяснить какие формулировки лучше использовать. Наиболее подходящими формулировками в данном случае являются: «Как на Ваш взгляд лучше поступить?», «Что мне лучше сделать в сложившейся ситуации?», «Какие пути решения имеются?». Данные формулировки можно использовать и при электронной переписке с взяткополучателем, если последний избегает встречи или не имеет такой возможности. Исключаются прямые вопросы, постановка которых может вызвать подозрение взяткополучателя, например: «Сколько я Вам буду должен?». Также взяткодателя необходимо научить пользоваться техническими средствами фиксации разговора с предполагаемым взяткополучателем¹⁰.

После окончания встречи взяткодатель доставляется в оперативное подразделение, где, в присутствии понятых, передает обратно технические средства, с помощью которых фиксировался разговор между ним и взяткополучателем. Полученные в ходе встречи сведения могут быть оформлены результатом оперативно-розыскного мероприятия

⁹ Оперативный эксперимент. // Кушнир И. В. Оперативно-розыскная деятельность. 2010. Режим доступа: Институт экономики и права Ивана Кушнирова: [сайт]. URL: <https://be5.biz/pravo/o001/30.html> (дата обращения: 10.05.2021).

¹⁰ Долинин В. Н. Особенности тактической операции «Задержание с поличным» при расследовании взятничества // Российский юридический журнал. 2015. № 3 (102). С. 176.

«Наблюдение»¹¹. Основная цель данного мероприятия заключается в слежении и фиксации действий и разговоров лиц, подозреваемых в преступной деятельности, а также в получении информации об объектах оперативного интереса.

Также при подготовке оперативного эксперимента, в условиях предполагаемой реализации взяткополучателем преступного умысла на получение взятки, осуществляемой под контролем оперативных сотрудников производится переписывание денежных купюр, их копирование, нанесение на предмет взятки химических или радиоизотопных меток, о чем составляется соответствующий акт с участием специалиста¹².

Завершающим элементом в комплексе оперативно-розыскных мероприятий, осуществляемых в целях документирования факта взяточничества, будет являться задержание с поличным взяткополучателя. Безусловно, что место встречи взяткодателя и взяткополучателя, непосредственная передача предмета взятки, действия взяткополучателя с предметом взятки, задержание взяткополучателя после

получения взятки, также по возможности должны осуществляться с проведением видеофиксации¹³.

Параллельно с задержанием лица с поличным (в практической деятельности значительно раньше) к проводимой операции привлекается следователь, который возбуждает уголовное дело, процессуально оформляет задержание взяткополучателя, определяет дальнейшие следственные и процессуальные действия по проведению расследования и доказыванию причастности лица к совершению выявленного преступления, которые, несмотря на то, что представляют определенный интерес и для теории и для практики, все же не являются предметом рассмотрения данной статьи.

При этом необходимо отметить, что следы, обнаруженные на взяткополучателе, свидетельствующие о его взаимодействии с предметом взятки будут иметь важное и доказательственное и криминалистическое значение¹⁴.

Таким образом, рассмотренные в работе аспекты позволяют выделить следующие особенности выявления и документирования фактов

¹¹ Правовые основы проведения оперативно-розыскных мероприятий в целях выявления и документирования получения взяток : учебно-методическое пособие / М. Л. Родичев [и др.]. СПб.: ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации», 2018. С. 26.

¹² Кузбагарова Е. В. Методика расследования взяточничества: Фондовая лекция. СПб.: Санкт-Петербургский университет МВД России, 2014.

¹³ Симакова А. В., Керимов М. А. Особенности задержания с поличным по делам о взяточничестве // Научный электронный журнал «Меридиан». 2020. № 2 (36). С. 492.

¹⁴ Христинина Е. В. Особенности изучения следов преступления при расследовании взяточничества в сфере высшего образования // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2018. Том 4, № 4. С. 150.

взяточничества при осуществлении оперативно-розыскной деятельности и использовании информационных технологий.

При поиске латентных (неизвестных фактов) взяточничества следует уделять значительное внимание наличию поисковых признаков, указывающих (присущих) на возможность подготовки или совершения рассматриваемого вида преступления. Проведение проверки лиц, по фактам предполагаемого взяточничества (готовящегося, совершаемого, совершенного) целесообразно связывать с изучением профилей проверяемых лиц в социальных сетях, установлением их связей и характера отношений.

В рамках оперативного изучения проверяемых лиц, необходимо обращать внимание на исследование различных аспектов деятельности данного лица (в первую очередь, связанных с исполнением им профессиональных обязанностей).

При подготовке и проведении оперативно-розыскных мероприятий сотрудникам оперативных подразделений необходимо выявлять и привлекать лиц, оказывающих содействие органам, осуществляющим оперативно-розыскную деятельность, имеющих возможности получения оперативно-значимой информации по интересующим оперативных сотрудников направлениям.

При выявлении в ходе осуществления оперативно-розыскной деятельности взяточдателя необходимо определить возможные способы установления с ним необходимого контакта и проведения

работы, направленной на оказание помощи оперативным сотрудникам в выявлении взяточполучателя и документировании осуществляемых последним преступных действий.

Правильная организация и умелое проведение опроса предполагаемого взяточдателя, позволит установить факты и обстоятельства, известные опрашиваемому лицу и способствующие принятию оперативными сотрудниками верных тактических решений по проведению комплекса оперативно-розыскных мероприятий в целях решения задач по выявлению, пресечению и раскрытию конкретного факта взяточничества.

При документировании преступных действий взяточполучателя необходимо привлекать все возможности оперативно-розыскных органов, в том числе по использованию современных информационных технологий, проведению оперативно-технических мероприятий, позволяющих получать сведения, содержащиеся в различных информационных системах и проходящих по различным каналам связи.

Проведение оперативно-розыскных мероприятий по выявлению и документированию фактов взяточничества в обязательном порядке должно соответствовать основаниям и условиям их проведения, а оформляемые надлежащим образом результаты оперативно-розыскной деятельности позволят использовать их в доказывании по уголовным делам, в соответствии с положениями

уголовно-процессуального законодательства Российской Федерации и	совершивших преступления. данной лиц,	вид
---	--	-----

Список литературы

1. Долинин В. Н. Особенности тактической операции «Задержание с поличным» при расследовании взяточничества // Российский юридический журнал. 2015. № 3 (102).
2. Карагодин В. Н. Методика расследования должностных преступлений: учебное пособие / В. Н. Карагодин, Н. Б. Вахмянина. 2-е изд. Екатеринбург, 2013.
3. Коломиец А. В. К вопросу о методике расследования современных способов совершения взяточничества с использованием мессенджеров / А. В. Коломиец, Э. Р. Ибляминова // Научный электронный журнал «Меридиан». 2020. № 4 (38).
4. Криминалистика в 3 ч. Часть 1 : учебник для вузов / Л. Я. Драпкин [и др.]; ответственный редактор Л. Я. Драпкин. 2-е изд., испр. и доп. Москва: Издательство Юрайт, 2019. 246 с. Режим доступа: ЭБС Юрайт [сайт]. URL: <https://urait.ru/bcode/434587>.
5. Кузбагарова Е. В. Методика расследования взяточничества: Фондовая лекция. СПб.: Санкт-Петербургский университет МВД России, 2014. 29 с.
6. Начальная профессиональная подготовка и введение в специальность: правоохранительная деятельность: учебник для среднего профессионального образования / Д. В. Бахтеев [и др.]; ответственный редактор Д. В. Бахтеев. Москва: Издательство Юрайт, 2019. 369 с. Режим доступа: ЭБС Юрайт [сайт]. URL: <https://urait.ru/bcode/442093>.
7. Оперативный эксперимент. // Кушнир И. В. Оперативно-розыскная деятельность. 2010. Режим доступа: Институт экономики и права Ивана Кушнера: [сайт]. URL: <https://be5.biz/pravo/o001/30.html>.
8. Павличенко Н. В. Негласность в оперативно-розыскной деятельности / Н. В. Павличенко, А. С. Самоделкин // Вестник Волгоградской академии МВД России. 2012. № 3 (22).
9. Правовые основы проведения оперативно-розыскных мероприятий в целях выявления и документирования получения взяток : учебно-методическое пособие / М. Л. Родичев [и др.]. СПб.: ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации», 2018. 145 с.
10. Симакова А. В. Особенности задержания с поличным по делам о взяточничестве / А. В. Симакова, М. А. Керимов // Научный электронный журнал «Меридиан». 2020. № 2 (36).
11. Христинина Е. В. Особенности изучения следов преступления при расследовании взяточничества в сфере высшего образования // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2018. Том 4, № 4.

12. Христинина Е. В. Особенности расследования получения взятки в системе высшего образования: дис. ... канд. юрид. наук. 2016.

Ildus F. Gaskarov

PhD (Law), Associate Professor,
Associate Professor of the Department of Criminalistics,
Ural State Law University
(Yekaterinburg, Russian Federation)
madagaskar.15@mail.ru

Danil S. Efimov

Student,
Ural State Law University
(Yekaterinburg, Russian Federation)
danilefimov00@mail.ru

SPECIAL ASPECTS OF ASCERTAINMENT AND DOCUMENTATION OF FACTS OF BRIBETAKING DURING THE IT POLICE OPERATIONS

Abstract: This article discusses the special aspects of identifying and documenting the facts of bribery. Particular attention is paid to the problems of law enforcement in the border of the implementation of police operations. The article also discusses operative investigations activity related to the use of information technology.

Keywords: bribery, police operations, operative search, operative investigations activity, information technology.

УДК 343.98

Долинин Владимир Николаевич

Кандидат юридических наук, доцент, доцент кафедры криминалистики,
Уральский государственный юридический университет
(г. Екатеринбург, Российская Федерация)
dvn1952@gmail.com

Шалудько Юлия Алексеевна

Магистрант,
Уральский государственный юридический университет
(г. Екатеринбург, Российская Федерация)
shaly7528@gmail.com

ИСПОЛЬЗОВАНИЕ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ В РАССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Аннотация: В настоящее время в связи с массовой компьютеризацией в России появились преступления в сфере компьютерной информации. Преступления, связанные с использованием компьютерных технологий, представляют серьезную угрозу и причиняют значительный материальный ущерб как отдельным государственным и коммерческим организациям, так и государству в целом. В представленной статье рассматриваются понятие и содержание криминалистической характеристики компьютерных преступлений, анализируются отдельные элементы этой категории, приводится классификация способов совершения различных учеными. Особое внимание уделяется описанию некоторых элементов исследуемых преступлений, высказываются некоторые предложения по совершенствованию качества расследования компьютерных преступлений.

Ключевые слова: криминалистическая характеристика, компьютерные преступления, способы совершения преступлений, классификация, расследование преступлений.

Для цитирования:

Долинин В. Н. Использование криминалистической характеристики в расследовании компьютерных преступлений / В. Н. Долинин, Ю. А. Шалудько // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 361–370.

В настоящее время одним из следствий массовой компьютеризации в России явились преступления в сфере компьютерной информации. Интеграция современных

информационных технологий практически во все области человеческой деятельности привела к тому, что с помощью компьютерных средств и систем совершаются

различные преступления. Компьютерные технологии используются с целью: фальсификации платежных документов; хищения наличных и безналичных денежных средств путем перечисления на фиктивные счета; отмыwania денег; вторичного получения уже произведенных выплат; совершения покупок с использованием фальсифицированных или похищенных электронных платежных средств; продажи секретной информации и проч. Преступления, сопряженные с использованием компьютерных технологий, представляют серьезную угрозу для любой располагающей компьютерной техникой организации и причиняют значительный материальный ущерб. Преступления, совершаемые с использованием компьютерных средств и систем, принято называть **компьютерными преступлениями**. Эта дефиниция должна употребляться не в уголовно-правовом аспекте, где это только затрудняет квалификацию деяния, а в криминалистическом, поскольку связана не с квалификацией, а именно со способом совершения и сокрытия преступления и, соответственно, с методикой его раскрытия и расследования.

В действующем Уголовном Кодексе РФ преступлениям в данной сфере относят составы, перечисленные в главе 28. Данные преступления довольно распространены. По данным статистики МВД о состоянии преступности за 2020 год, 8,4 % всех зарегистрированных преступлений за отчетный период совершены с

использованием компьютерных и телекоммуникационных технологий. Например, в Свердловской области в 2018 году зарегистрировано 10 компьютерных преступлений, в 2019 – 30, а в 2020 уже 54.

Исходной информационной базой для расследования указанных преступлений является криминалистическая характеристика. В содержание криминалистической характеристики преступлений в сфере компьютерных преступлений, по нашему мнению, должны входить следующие структурные элементы: место совершения преступления (обстановка); способы совершения преступления; орудие (средства) совершения преступления; механизм следообразования; сведения о личности потерпевшего; мотивы; сведения о личности преступника.

Место совершения преступления. Местом совершения преступлений в сфере компьютерной информации принято считать место совершения общественно опасного деяния. Так, преступление, предусмотренное ст. 272 УК РФ, признается оконченным, когда наступили последствия неправомерного доступа к охраняемой законом компьютерной информации в виде уничтожения, блокирования, модификации или копирования данной информации. Местом совершения преступления необходимо признать место совершения наступления последствий. Преступление, предусмотренное ст. 273 УК РФ, признается оконченным с момента создания, распространения или использования вредоносной

компьютерной программы или иной компьютерной информации независимо от наступления последствий; местом вовершения следует признавать место создания, распространения или использования компьютерной программы или иной компьютерной информации. Это могут быть нежилые или жилые помещения, чаще всего съемные квартиры.

Способы совершения преступления. В юридической литературе имеется несколько классификаций способов совершения преступлений в сфере компьютерной информации, но нельзя считать каждую из них абсолютно точной, так как все они не являются исчерпывающими. Например, Ю. М. Батурин предлагает общую классификацию способов: «методы перехвата; методы несанкционированного доступа и методы манипуляции»¹ с последующим подробным описанием. С. П. Кушнаренок выделяет следующие способы: «модификации компьютерных программ с целью проводки подложных электронных документов для создания резерва денежных средств с их последующим перечислением на счета юридических и физических лиц, обналичиванием и изъятием; изменения программ по начислению заработной платы и зачисления ее на лицевые счета сотрудников с автоматическим

списанием части наличных сумм на свой счет и на счета соучастников; произведения незаконных начислений денежных выплат с последующим их хищением путем подделки подписи получателей в оформленных платежных документах; создания файлов с вымышленными вкладчиками, зачисления и проводки по их счетам фиктивных денежных сумм с последующим переводом на свой счет и их хищением; получения в базах данных кредитно-финансовых учреждений номеров банковских карт и ПИН-кодов с последующим использованием в расчетах денежных средств клиентов банка; искажения реквизитов электронных платежных документов, касающихся адресата получателя денег, с переводом их на свой счет или счета соучастников; занижения суммы выручки торговых предприятий путем установки специальных вредоносных программ на контрольно-кассовые аппараты, являющиеся ЭВМ, для совершения налоговых преступлений и хищений»². Д. С. Будаковский разделяет все способы совершения на две группы: к первой группе способов относятся способы непосредственного воздействия на компьютерную информацию, ко второй – способы опосредованного (удаленного) воздействия на компьютерную информацию³. Среди наиболее часто встречающихся способов можно назвать: распространение

¹ Батурин Ю. М. Компьютерная преступность и компьютерная безопасность. М., 1991. С. 19–22.

² Кушнаренок С. П. Методика расследования преступлений в сфере высоких технологий:

лекция. Краснодарский университет МВД РФ, 2008. С. 12.

³ Будаковский Д. С. Способы совершения преступлений в сфере компьютерной информации // Российский следователь. 2011. № 4. С. 2–4.

вредоносных программ, подбор нужного пароля, в том числе с использованием специальных программ автоматического подбора, получение паролей доступа обманным путем, подключение к линии связи законного пользователя и получение тем самым доступа к его системе, использование различных программных средств специального назначения, направленных на восстановление удаленных файлов.

Орудия (средства) совершения преступления. Преступления в сфере компьютерной информации всегда совершаются с помощью средств компьютерной техники. Понятие этих средств является комплексным, включающим в себя компьютеры в различных вариантах их исполнения (ноутбуки, планшеты, смартфоны, и т. д.), компьютерные технологии (беспроводные Wi-Fi, Bluetooth, 3G, WiMAX и др.), а также компьютерное программное обеспечение, находящееся в открытом, запрещенном или ограниченном обороте и имеющее различное назначение (разрешенные и бесплатно распространяемые программы, например, Opera, Mozilla, Firefox, вредоносные программы, например, SpyEye, Zeus, Carberp и т. д.). Следует отметить, что в настоящее время главную роль при совершении компьютерных преступлений выполняет программное обеспечение, а не аппаратные средства, которые обычно не представляют опасности.

Как показывает следственная практика, в «большинстве случаев компьютерные преступления совершаются путем удаленного доступа по телекоммуникационным сетям с помощью обычной компьютерной техники, которую устанавливается специальное программное обеспечение»⁴.

Механизм следообразования. В юридической литературе можно встретить понятия «виртуальные следы», «цифровые следы» при описании механизма следообразования при совершении преступлений в сфере компьютерной информации.

Виртуальные следы представляют собой следы совершения любых действий в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей. В. Мещеряков под виртуальными следами понимает «любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации. Данные следы занимают условно промежуточную позицию между материальными и идеальными следами»⁵.

А. Г. Волеводз выдвинул классификацию виртуальных следов на основании непосредственного физического носителя следов:

1. следы на жестком диске,

⁴ Поляков В. В. обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики //

Известия Алтайского государственного университета. 2013 № 2. С. 114–116.

⁵ Мещеряков В. А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. 2013. № 5 (10). С. 265–269.

магнитной ленте, оптическом диске, на дискете;

2. следы в оперативных запоминающих устройствах ЭВМ, периферийных устройствах, компьютерных устройствах связи и сетевых устройствах;

3. следы в проводных и других электромагнитных системах и сетях связи⁶.

Л. Б. Красновой предложена классификация «виртуальных следов» по механизму следообразования на первичные и вторичные следы. Первичные формирует непосредственное воздействие пользователя с использованием какой-либо информационной технологии, а вторичные – результат воздействия технологических процессов без участия человека⁷.

В. Б. Вехов предлагает понятие «электронно-цифровой след», под которым понимает «любую криминалистически значимую компьютерную информацию, то есть сведения, находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе либо передающиеся по каналам связи посредством электромагнитных сигналов»⁸.

Е. Р. Россинская шире трактует это понятие: «цифровой след представляет собой

криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи. Цифровые следы отличаются высокой скоростью трансформации, легко уничтожаются и модифицируются, могут быть представлены практически бесконечным количеством копий, легко распространяются в компьютерных сетях и доступны в любой точке, где имеется подключение к сети Интернет»⁹.

Мотивы. Мотивами совершения компьютерных преступлений, как показали исследования зарубежных и российских исследователей, являются следующие: корыстные мотивы; политические цели; исследовательский интерес; хулиганские; месть.

«Для подавляющего большинства преступлений характерны корыстные мотивы — 52 % всех компьютерных преступлений; с разрушением и уничтожением средств компьютерной техники сопряжено 16 % преступлений, с подменой исходных данных — 12 %, с хищением данных и программ — 10 %, с хищением услуг — 10 %»¹⁰.

⁶ Волеводз А. Г. Противодействие компьютерным преступлениям. М., 2002. С. 159–160.

⁷ Краснова Л. Б. Компьютерные объекты в уголовном процессе и криминалистике: автореф. дис. ... канд. юрид. наук. Воронеж, 2005. С. 17.

⁸ Вехов В. Б. Криминалистическое учение о компьютерной информации и средствах ее

обработки: автореф. дис. ... д-ра юрид. наук. Волгоград, 2008. С. 45.

⁹ Е. Р. Россинская Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О. Е. Кутафина. 2019. № 5.

¹⁰ Старостина Е. В., Фролов Д. Б. Защита от компьютерных преступлений и

Исследовательский интерес преобладает у молодых людей, осуществляющих неправомерный доступ к компьютерной информации различных правообладателей: физических лиц, коммерческих структур, государственных учреждений и ведомств. Чем более защищена информация ведомства, тем настойчивее осуществляются хакерские атаки, в том числе по предварительному сговору группами преступников, объединяющихся путем общения через глобальную сеть, иногда даже из различных стран.

Мотивами мести руководствуются 12,9 % преступников. Чаще всего пытаются отомстить за недооценку их личности и профессионализма или за необоснованное увольнение с работы. Например, гражданка Г., подлежащая увольнению по сокращению штатов из городского управления жилищно-коммунальных услуг г. Курчатова, недовольная этим фактом, решила осложнить работу подразделений городской администрации. Используя свое служебное положение, Г., занимавшая должность инженера-программиста, под разными предлогами получила доступ к ЭВМ пяти ЖКХ города и уничтожила программу «Квартплата»¹¹.

Сведения о потерпевшем. Потерпевших можно подразделить на три основные группы: собственники компьютерной системы; клиенты,

пользующиеся их услугами; иные лица.

Потерпевший, особенно относящийся к первой группе, часто неохотно сообщает (или вовсе не сообщает) правоохранительным органам о преступных фактах по следующим причинам: «из-за некомпетентности сотрудников правоохранительных органов в данном вопросе; нежелания раскрытия в ходе судебного разбирательства системы безопасности организации; боязни выявления собственных незаконных действий; боязни должностных лиц, что одним из итогов расследования станут выводы об их профессиональной непригодности (некомпетентности); из-за правовой неграмотности; из-за непонимания истинной ценности имеющейся информации и по другим причинам»¹².

Сведения о личности преступника. Личность преступника отличается целым рядом особенностей: четко формулирует любую профессиональную задачу; обладает развитым формально-логическим мышлением; постоянно использует компьютерный жаргон, малопонятный собеседнику.

Преступники в сфере компьютерной информации могут быть разделены на две возрастные группы: первая – 14–20 лет, вторая – с 21 года и старше. Представители первой возрастной группы – это

кибертерроризма. М.: Изд-во Эксмо, 2005. С. 26.

¹¹ Уголовное дело № 37298 // Архив Курчатовского городского суда Курской области. 2019.

¹² Криминалистика: учебник // под ред. Т. В. Аверьяновой [и др.]. 4-е издание. М.: Норма, 2013. С. 907.

старшие школьники или студенты младших курсов высших или средних специальных учебных заведений, которые активно ищут пути самовыражения и находят их, погружаясь в виртуальный мир компьютерных сетей. При этом чаще всего ими движет скорее любопытство и исследовательский интерес, нежели корыстные мотивы. К числу особенностей, указывающих на совершение компьютерного преступления лицами рассматриваемой категории, можно отнести: отсутствие целеустремленной, продуманной подготовки к преступлению; неприятие мер к сокрытию преступления; факты немотивированного озорства.

Компьютерные преступники, входящие во вторую возрастную группу, – «это вполне сформировавшиеся личности, обладающие высокими профессиональными и устойчивыми преступными навыками, а также определенным жизненным опытом. Совершаемые ими деяния носят осознанный корыстный характер, при этом, как правило, предпринимаются меры по противодействию раскрытию преступления. Преступления, которые носят серийный, многоэпизодный характер обязательно сопровождаются действиями по сокрытию. Это обычно высококвалифицированные специалисты с высшим математическим, инженерно-техническим или экономическим

образованием, входящие в организованные преступные группы и сообщества, прекрасно оснащенные технически (нередко специальной оперативной техникой). Особую опасность с точки зрения совершения преступлений в сфере компьютерной информации представляют профессионалы в области новых информационных технологий»¹³.

Профессор Р. С. Белкин всех компьютерных преступников разделяет на три группы:

- лица, владеющие специальными навыками в области управления ЭВМ и ее устройствами, а также специальными познаниями в области обработки информации в информационных системах в целом, знающие финансовые, бухгалтерские, информационные технологии. Ими совершаются хорошо продуманные и тщательно подготовленные преступления, в основном корыстные;
- лица, не обладающие серьезными познаниями в области программирования и компьютерной техники, имеющие лишь некоторые пользовательские навыки работы с ЭВМ. Их действия направлены на уничтожение, блокирование, модификацию, копирование ничем не защищенной информации;
- лица, имеющие психические отклонения. К их числу относят страдающих различными компьютерными фобиями. Эта категория заболеваний связана с нарушениями в информационном режиме человека под воздействием внешних или внутренних

¹³ Криминалистика: учебник // под ред. Т. В. Аверьяновой [и др.]. 4-е издание. М.: Норма, 2013. С. 906.

дестабилизирующих факторов как врожденного, так и приобретенного свойства¹⁴.

В следственной практике всех лиц, совершающих преступление в сфере компьютерной информации, разделяют на три группы:

1. Хакеры – профессиональные взломщики защиты компьютерных программ и создатели компьютерных вирусов, которых отличает высокий профессионализм в сочетании с компьютерным фанатизмом.

В зависимости от вида деятельности хакеры имеют следующие специализации:

а) крекеры (взломщики защиты программ от неоплаченного использования);

б) фриеры (используют альтернативные варианты оплаты телефонных услуг для обмана АТС);

в) кардеры (оплачивают свои расходы с чужих кредитных карточек);

г) сетевые хакеры (взломщики защиты провайдера) и др.

К признакам совершения преступлений в сфере компьютерной информации хакерами относятся оригинальность способа и отсутствие тщательной подготовки к преступлению и его сокрытию.

2. Психически больные лица, страдающие компьютерными фобиями (т. е. профессиональными информационными заболеваниями), которые уничтожают или повреждают компьютерную технику без наличия преступного умысла с частичной или полной потерей контроля над своими действиями.

3. Криминальные профессионалы – т. е. преступные группировки, преследующие политические цели; лица, занимающиеся промышленным шпионажем; группировки отдельных лиц, стремящихся к наживе. Преступления, совершаемые ими в сфере компьютерной информации, носят серийный, многоэпизодный характер, совершают многократно, обязательно с применением мер по сокрытию преступления.

Одной из проблем расследования компьютерных преступлений является тот факт, что следователи не проводят анализ содержания криминалистической характеристики, не используют ее в ходе следствия. В результате определяют не оптимальные направления поиска доказательственной информации и проводят некачественные расследования. Так, например, в 2020 году следователями ГСУ ГУ МВД РФ по Свердловской области возбуждено 54 уголовных дел по признакам преступления в сфере компьютерной информации, а в суд направлено лишь 30. Остальные уголовные дела были прекращены по различным основаниям, в том числе из-за недоказанности. Представляется, что использование криминалистической характеристики целесообразно по следующему алгоритму:

1. На основе анализа выявить закономерные многоструктурные взаимосвязи между элементами криминалистической характеристики указанных преступлений особенно:

¹⁴ Криминалистика: учебник / под ред. Р. С. Белкина. М., 1999. С. 950–951.

способы совершения → механизм
слепообразования → мотив →
личность преступника.

2. Построить типовые версии о личности преступника и составить план расследования.

3. Определить наиболее оптимальные направления расследования, составить и реализовать комплекс (программу) следственных действий и оперативно-розыскных мероприятий.

Другой проблемой является отсутствие у следователей надлежащих знаний, умений и навыков по расследованию

компьютерных преступлений. Опыт расследования приходит со стажем работы. Необходимо в юридических ВУЗах страны разработать и внедрить спецкурс «Методика расследования компьютерных преступлений». Такой спецкурс несколько лет успешно реализуется в Краснодарском университете МВД РФ. Реализация вышеуказанных предложений, по нашему мнению, позволит решить отмеченные проблемы и будет способствовать качественному расследованию компьютерных преступлений.

Список литературы

1. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность. М., 1991. 160 с.
2. Будаковский Д. С. Способы совершения преступлений в сфере компьютерной информации // Российский следователь. 2011. № 4. С. 2–4.
3. Вехов В. Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: автореф. дис. ... д-ра юрид. наук. Волгоград, 2008. 45 с.
4. Волеводз А. Г. Противодействие компьютерным преступлениям. М., 2002.
5. Краснова Л. Б. Компьютерные объекты в уголовном процессе и криминалистике: автореф. дис. ... канд. юрид. наук. Воронеж, 2005.
6. Криминалистика: учебник / под ред. Т. В. Аверьяновой [и др.]. 4-е издание. М.: Норма, 2013.
7. Криминалистика: учебник / под ред. Р. С. Белкина. М., 1999.
8. Кушнаренко С. П. Методика расследования преступлений в сфере высоких технологий: лекция. Краснодарский университет МВД РФ, 2008.
9. Мещеряков В. А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. 2013. № 5 (10). С. 265–269.
10. Поляков В. В. обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. 2013. № 2. С. 114–116.
11. Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О. Е. Кутафина. 2019. № 5. С. 31–44.
12. Старостина Е. В. Защита от компьютерных преступлений и кибертерроризма / Е. В. Старостина, Д. Б. Фролов. М.: Изд-во Эксмо, 2005.

Vladimir N. Dolinin

PhD (Law), Associate Professor,
Associate Professor of the Department of Criminalistics,
Ural State Law University
(Yekaterinburg, Russian Federation)
dvn1952@gmail.com

Yulia A. Shaludko

Graduate student,
Ural State Law University
(Yekaterinburg, Russian Federation)
shaly7528@gmail.com

THE USE OF FORENSIC CHARACTERISTICS IN THE INVESTIGATION OF COMPUTER CRIMES

Abstract: Currently, in connection with mass computerization in Russia, there are crimes in the field of computer information. Crimes related to the use of computer technologies create a serious threat and cause significant material damage to individual state and commercial organizations, as well as to the state as a whole. The article deals with the concept and content of the criminalistic characteristics of computer crimes, analyzes the individual elements of this category, and provides a classification of the methods of committing various crimes. Special attention is paid to the description of some elements of the investigated crimes, and some suggestions are made to improve the quality of investigation of computer crimes.

Keywords: criminalistic characteristics, computer crimes, methods of committing crimes, classification, investigation of crimes.

Коломинов Вячеслав Валентинович

Кандидат юридических наук, доцент кафедры криминалистики, судебных экспертиз и юридической психологии Института государства и права, Байкальский государственный университет
(г. Иркутск, Российская Федерация)
KolominovVV88@gmail.com

СЛЕДСТВЕННАЯ СТРАТЕГИЯ В РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация: Мир инновационных технологий диктует свои новые общеобязательные правила поведения в информационной среде. Но всегда найдутся делинквенты, которые будут преследовать свои преступные цели в сети Интернет. Для своевременного предотвращения и полного раскрытия преступлений обычных средств и круга действий, обозначенного законом, следователю уже не хватает. Вместе с тем стоит отметить, что назревает необходимость в пересмотре нормативных актов, регулирующих действия следственных органов. Статья представляет собой исследование новых методов и способов, которые должны знать правоохранители, чтобы своевременно принимать оправданные следственные решения для сохранения важнейших улик, которые могут быть положены в доказательную базу. В статье автор поднимает вопросы, связанные с преступлениями с применением современных информационных и инновационных технологий. Сейчас такие виды противоправных действий носят название киберпреступления. Как и сами действия преступников, так и действия следователей по раскрытию и предотвращению носят особенный характер. Недостаток квалифицированных кадров среди следователей, дознавателей и оперативных сотрудников сказывается негативно на динамике раскрытия преступлений. И привлечение узких специалистов не всегда оправданная мера, так как большое количество доказательной базы в силу особенности исчезает практически сразу после совершения деяния. В таком случае возникает оправданный вопрос, какие оперативные меры может самостоятельно произвести следователь. Актуальность статьи подчеркивается современными методами решения вышеуказанных проблем, анализом новых видов киберпреступлений и подробным описанием способов совершения. Автор использовал аналитический и формально-юридический методы исследования. Цель написания статьи – повышение уровня информированности среди всех сотрудников органов безопасности о современных способах мошеннических действий в сети Интернет и цифровой среде. Для реализации поставленных целей автор ставит перед собой задачу изучить актуальные методы противодействия киберпреступности в крупнейших профильных источниках. Приводится краткий анализ возможных первоочередных мер в следственной стратегии.

Ключевые слова: компьютерные преступления, уголовное право, киберпреступления, фишинг, кликджекинг, информационные технологии.

Для цитирования:

Коломинов В. В. Следственная стратегия в расследовании киберпреступлений // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 371–375.

Преступность в сфере высоких технологий относительно преступлений в других областях «молода», однако существенный рост количества фактов мошеннических действий с использованием высоких технологий predetermined законодательное закрепление и выделение отдельной нормы, устанавливающей ответственность за хищения подобного рода. Компьютер представляет собой уникальное устройство, способное упростить жизнь его пользователей, выполнить сложные вычислительные процессы и просто является неотъемлемым атрибутом современного человека. По мере модернизации и совершенствования техники, видоизменяются и усложняются общественные отношения, а, следовательно, нарушения, которые происходят в обществе, начинают приобретать новую, ранее неизвестную форму.

Нужно отметить, что допрос по уголовным делам при расследовании киберпреступлений имеет определенную специфику. Привлечение специалистов к проведению ряда следственных действий может помочь устранить недостатки в знаниях и навыках у следователя. Однако в некоторых случаях присутствие специалиста в том варианте, в котором высказываются ученые-криминалисты может быть неоправданно. В арсенале у следователя должен быть набор

превентивных мер, к которым он может прибегнуть в оперативном порядке без привлечения специалистов в области информатики и техники. Тактика проведения следственных действий зависит в первую очередь напрямую от заявителя. Является ли он частным лицом, юридическим. Или же противоправные действия были допущены в отношении неопределенной группы лиц. Рассмотрим некоторые из них.

В последние годы участились мелкие киберпреступления в отношении граждан. И чаще всего они остаются неучтенными по вполне понятным причинам. Взлом личной переписки в соцсетях со всеми подробностями личной жизни и расследование по такому делу может ударить по репутации гражданина, и он не решается идти с заявлением в органы правопорядка. Но когда идет речь о списывании сумм на мошеннических сайтах без получения оплаченного товара или услуги, граждане охотно обращаются и помогают в расследовании. Среди мелких частных преступлений большую часть занимают фишинг и кликджекинг.

Фишинг (буквально: ловить на удочку) – это способ перенаправить человека с помощью электронного письма или сообщения на подставной сайт, который имеет все схожие элементы с официальными сайтами

известных компаний¹. Очень популярен вид подобного мошенничества на известных площадках типа «Авито» или «Юла». Ни о чем не подозревающий покупатель соглашается перевести деньги за товар, и тогда ему в чат продавец присылает ссылку на сервис типа «Яндекс.Доставка», убеждая провести перевод денег, чтобы оформить доставку, через популярный ресурс. Как правило, мошенники без труда могут за пару часов написать лендинг, который будет иметь все атрибуты сайта-оригинала – логотип, цвета, разметку и стили. Загрузить его на сомнительный хостинг вне пределов РФ и добавить платежное окно также не представляет сложности. И все это, конечно, не имеет отношение к официальной компании. Жертва теряет деньги и понимает об этом нескоро. В этом случае в первую очередь стоит обратиться в техподдержку портала, где производилось общение в чате, и где было размещено объявление мошенника. Как правило, они реагируют быстро и удаляют аккаунт. Но в таком случае найти преступников становится сложнее, так как и сами мошенники быстро удаляют сайт и аккаунт на хостинге. Если поддельный сайт еще не удален, можно без помощи IT специалистов быстро установить, где хостится сайт. Сейчас много официальных интернет-ресурсов, предлагающих подобные услуги. Официальный запрос в хостинг поможет установить многие элементы: IP адрес самого сайта и владельца

аккаунта, с которого производился фишинг. А в некоторых случаях добросовестные и крупные игроки на рынке хостинговых услуг в обязательном порядке требуют заполнить личные данные, среди которых и email пользователя.

В случае кликджекинга (click – «нажатие» и hijack – «захватить») большую сложность играет тот факт, что поверх официального популярного ресурса, точнее его кнопок и полей для заполнения личных данных, может быть установлен невидимый html-элемент iframe, который содержит невидимые кнопки и поля, написанные при помощи стиля opacity. Нажимая на такую кнопку, клики перехватываются и используются для выполнения любого из действий, например, записи видео на веб-камеру². Изъятие компьютера в таком случае будет оправданной первоочередной мерой. Производить анализ содержимого следует с привлечением специалистов. Сложные технические и программные особенности содержимого, как на носителе, так и в самих файлах, определенно представляют трудность для изучения следователями с непрофильным образованием. А способных специалистов среди внутренних кадров очень сложно найти. В первую очередь стоит исследовать историю браузерных переходов и установленных расширений и программ. Если имеется лицензионная антивирусная программа, стоит привлечь их специалистов, так как в

¹ What Is Phishing? // Phishing.org [website]. URL: <https://www.phishing.org/what-is-phishing> (accessed: 10.02.2021).

² Мышь в ловушке. Что такое кликджекинг и как защитить свои клики // Эксплойт [сайт]. URL: <https://exploit.media/security/clickjacking/> (дата обращения: 10.02.2021).

большинстве случаев перехваты должны блокироваться антивирусом.

Если идет речь о фирмах, в отношении которых были произведены хакерские атаки, утечка крупных средств со счетов или иные преступления, то среди первоочередных мер стоят выемка и опрос. И если выемка возможна только в определенных законом случаях, то опрос свидетелей – вполне законная превентивная мера. В первую очередь стоит установить субординацию пользователей компьютерной сети, у кого есть права администратора, и кто на самом деле осуществляет функции системного администратора. А это могут быть разные лица. Существенная разница в трудовых обязанностях, которые лежат на системном администраторе и его объективной возможности регулировать деятельность пользователей, и возможности доступа к скачиванию любых программ, в том числе и вредоносных ПО, плагинов, расширений, которая есть у фактического администратора компьютер, а в сети. Особенный интерес представляют файлы с расширением .log. Они являются

доказательством, когда необходимо выявить проблемы, нарушения безопасности и оценить возможность проникновения³. Сейчас эти файлы присутствуют не только на носителях систем или сервере, но и во многих программах.

Если речь идет о фирме, в отношении которой имеются подозрения в совершении кибератак или использовании незаконных программ для совершения незаконных сделок, например, на рынке ценных бумаг или незаконных переводов с целью сокрытия конечного бенефициара, то самыми результативными мерами будут санкционированная на законодательном уровне незамедлительная выемка всех технологических носителей, включая флеш-накопители, анализ и осмотр с привлечением квалифицированных специалистов.

Резюмируя, стоит отметить, что даже в самых сложных случаях сейчас имеется достаточно обычных гражданских доступных средств для установления причинно-следственной связи в делах по киберпреступлениям.

Список литературы

1. What Is Phishing? // Phishing.org [website]. URL: <https://www.phishing.org/what-is-phishing>.
2. Мышь в ловушке. Что такое клиджекинг и как защитить свои клики // Эксплойт [сайт]. URL: <https://exploit.media/security/clickjacking/>.
3. What is a .log file? // Reviversoft.com [website]. URL: <https://www.reviversoft.com/file-extensions/log>.

³ What is a .log file? // Reviversoft.com [website]. URL: <https://www.reviversoft.com/file-extensions/log> (accessed: 10.02.2021).

Vyacheslav V. Kolominov

PhD (Law), Associate Professor of the Department of Criminalistics, Forensic Expertise
and Legal Psychology of Institute of State and Law,
Baikal State University
(Irkutsk, Russian Federation)
KolominovVV88@gmail.com

INVESTIGATIVE STRATEGY IN THE INVESTIGATION OF CYBERCRIME

Abstract: The world of innovative technologies dictates its new mandatory rules of behavior in the information environment. But there will always be delinquents who will pursue their criminal goals on the Internet. For the timely prevention and full disclosure of crimes, the usual means and the range of actions specified by the law are no long enough for the investigator. At the same time, it is worth noting that there is a need to review the regulations governing the actions of investigative bodies. The article is a study of new methods and methods that law enforcement officers should know in order to make timely justified investigative decisions in order to preserve the most important evidence that can be put into the evidence base. In the article, the author raises issues related to crimes involving the use of modern information and innovative technologies. Now such types of illegal actions are called cybercrime. Both the actions of the criminals themselves and the actions of the investigators to detect and prevent them are of a special nature. The lack of qualified personnel among investigators, interrogators and operational staff has a negative impact on the dynamics of crime detection. And the involvement of narrow specialists is not always a justified measure, since a large amount of evidence base disappears almost immediately after the commission of the act. In this case, a reasonable question arises as to what operational measures the investigator can independently take. The relevance of the article is emphasized by modern methods of solving the above problems, the analysis of new types of cybercrimes and a detailed description of the methods of commission. The author used analytical and formal-legal methods of research. The purpose of this article is to raise awareness among all security officials about modern methods of fraudulent activities on the Internet and in the digital environment. To achieve these goals, the author sets himself the task of studying current methods of countering cybercrime in the largest specialized sources. A brief analysis of possible priority measures in the investigative strategy is provided.

Keywords: computer crimes, criminal law, cybercrime, phishing, clickjacking, information technology.

Никитина Елена Викторовна

Кандидат юридических наук, доцент кафедры судебной деятельности и
уголовного процесса,

Уральский государственный юридический университет

(г. Екатеринбург, Российская Федерация)

nick2210@yandex.ru

**ЭЛЕКТРОННЫЕ СООБЩЕНИЯ КАК ОБЪЕКТ ПРОЦЕССУАЛЬНОГО
ОСМОТРА**

Аннотация: В статье обращается внимание на отсутствие в уголовно-процессуальном законе определения такого понятия, как «электронные сообщения». С учетом анализа Федерального закона от 27 июля 2006 г. № 149-ФЗ (в ред. от 30.12.2020) «Об информации, информационных технологиях и о защите информации» предлагается дополнить статью 5 УПК РФ следующими понятиями: «электронное сообщение» и «информационно-телекоммуникационная сеть». Исследуется проблема процессуального осмотра электронных сообщений с точки зрения соблюдения конституционных прав граждан. Приводится позиция Конституционного Суда РФ, данная им в определении от 25 января 2018 года № 189-О. Излагаются различные толкования этого определения, предложенные в специальной литературе. Представлено собственное видение проблемы, а также позиции, занимаемой Конституционным Судом РФ.

Ключевые слова: электронные сообщения, информационно-телекоммуникационная сеть, электронные носители информации, процессуальный осмотр, судебное решение.

Для цитирования:

Никитина Е. В. Электронные сообщения как объект процессуального осмотра // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 376–381.

Прежде чем говорить о таком объекте осмотра, как электронные сообщения, следует определиться терминологически. Уголовно-процессуальный кодекс РФ не расшифровывает понятия «электронные сообщения». О них упоминается лишь в части 7 статьи 185 УПК РФ в том смысле, что следователь вправе по решению суда произвести осмотр и выемку

электронных сообщений или иных передаваемых по сетям электросвязи сообщений – при наличии достаточных оснований полагать, что сведения, содержащиеся в них, имеют значение для уголовного дела.

Вместе с тем, Федеральным законом от 27 июля 2006 г. № 149-ФЗ (в ред. от 30.12.2020) «Об информации, информационных технологиях и о защите информации»

электронное сообщение определяется как информация, переданная или полученная пользователем информационно-телекоммуникационной сети (пункт 10 статьи 2)¹. Информационно-телекоммуникационная сеть определена как технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (пункт 4 статьи 2)².

Анализ этих законодательных положений приводит к выводу о том, что к электронным сообщениям относятся и «иные передаваемые по сетям электросвязи сообщения». В связи с этим их упоминание в части 7 статьи 185 УПК РФ (наряду с электронными сообщениями) излишне.

Думается, электронными сообщениями следует считать письма, пересылаемые по электронной почте, личные сообщения в социальных сетях, переписку посредством

сервисов мгновенных сообщений (мессенджеров), а также сообщения, передаваемые посредством мобильной связи (SMS, MMS)³.

Отсутствие определенности в таких понятиях, как электронное сообщение и информационно-телекоммуникационная сеть, является упущением уголовно-процессуального законодательства. Представляется целесообразным внести их в статью 5 УПК РФ, раскрывающую основные понятия, используемые в Уголовно-процессуальном кодексе РФ.

Что касается осмотра электронных сообщений⁴, один из главных вопросов, встающих перед правоприменителем, – всегда ли такой осмотр требует судебного решения. С чем чаще всего сталкиваются следователи? С проблемой осмотра уже полученных абонентом электронных сообщений, имеющих на каком-либо электронном носителе информации⁵. Надо ли при изъятии такого электронного носителя информации в ходе, например,

¹ Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 № 149-ФЗ (в ред. ФЗ от 30.12.2020 № 530-ФЗ): принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобрен Советом Федерации 14 июля 2006 г. // Российская газета. 2006. 29 июля.

² Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 № 149-ФЗ (в ред. ФЗ от 30.12.2020 № 530-ФЗ): принят Гос. Думой Федер. Собр. Рос. Федерации 8 июля 2006 г.: одобрен Советом Федерации 14 июля 2006 г. // Российская газета. 2006. 29 июля.

³ Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с

использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / А. В. Аносов [и др.]. М.: Академия управления МВД России, 2019. Ч. 1. С. 89–94.

⁴ Вопросы выемки электронных сообщений не рассматриваются в рамках настоящей работы.

⁵ Долинин В. Н., Кабитова Ю. Р., Елькина П. С. Технологии собирания, исследования и использования электронно-цифровых доказательств // Технологии XXI века в юриспруденции: материалы Всероссийской научно-практической конференции (Екатеринбург, 24 мая 2019 года) / под ред. Д. В. Бахтеева. Екатеринбург: Уральский государственный юридический университет, 2019. С. 49–51.

осмотра места происшествия, обыска или выемки получать специальное судебное решение на осмотр имеющихся там электронных сообщений или в этом случае судебное решение не требуется?

В специальной литературе высказывалась точка зрения о том, что изъятие электронного устройства допустимо без судебного решения, однако осмотр любой хранящейся в нем информации возможен только по решению суда⁶.

Ответ на этот вопрос дал Конституционный Суд РФ в своем определении от 25 января 2018 года № 189-О⁷. Он разъяснил, что проведение осмотра с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения.

Такое разъяснение Конституционного Суда РФ вызвало неоднозначное толкование. По мнению К. Б. Калиновского, данное определение Конституционного Суда РФ следует понимать так, что судебное решение на осмотр

электронных сообщений требуется лишь в том случае, когда в правоотношениях участвует оператор связи. Именно он отвечает за соблюдение тайны электронной переписки. Если же оператор связи не участвует в правоотношениях, предварительный судебный контроль не нужен, поскольку следователь не вторгается в сам процесс обмена электронными сообщениями, не прибегает к использованию мощностей оператора связи. Иначе потребуются получать судебное решение и для изъятия переписки, передаваемой с нариском или «голубиной почтой»⁸.

С подобным толкованием позиции Конституционного Суда РФ согласны не все. Так, например, А. А. Хайдаров считает, что в определении Конституционного Суда РФ⁹ речь не идет о данном следователям праве знакомиться без судебного решения с электронной перепиской лица в ходе осмотра его телефона. В нем лишь подчеркивается, что телефоны (планшеты) и иные подобные цифровые устройства могут изыматься по уголовным делам с целью получения информации, находящейся в их электронной памяти. И для этого действительно не

⁶ Бикмиев Р. Г., Бурганов Р. С. Выемка и осмотр электронных устройств // Уголовное право. 2018. № 1. С. 131.

⁷ Определение Конституционного Суда РФ от 25.01.2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации» // Законы, кодексы, нормативные и судебные акты.

URL: <https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rf-ot-25012018-n-189-o/> (дата обращения: 10.05.2021).

⁸ Решение суда для фиксации переписки на смартфонах в ходе осмотра не нужно // Уголовный процесс. 2018. № 4. С. 7.

⁹ Автор перепутал два определения Конституционного Суда РФ с одной и той же датой (25.01.2018) и по жалобе одного и того же гражданина (Прозоровского Д. А.): анализировал определение № 189-О, а называл его определением № 193-О.

нужно судебного решения. Однако в памяти этих устройств имеется большое количество информации, которая может иметь отношение к уголовному делу, и только часть из этой информации охраняется законом. Поэтому, если гражданин считает, что нарушаются его конституционные права, он может обратиться в суд и оспорить законность проведенных следственных действий на том основании, что в протоколах этих следственных действий содержится информация, которая может быть получена только по судебному решению¹⁰.

Более правильной, однако, представляется точка зрения К. Б. Калиновского. Думается, Конституционный Суд РФ посчитал электронные сообщения (информацию, находящуюся в электронной памяти абонентских устройств, изъятых при производстве следственных действий), «иными документами» в том смысле, как их понимает уголовно-процессуальный закон (ст. 84 УПК РФ). Следовательно, их осмотр должен производиться по правилам осмотра «иных документов», оказавшихся в распоряжении следователя в результате производства какого-либо следственного действия, не требующего специального судебного решения на их осмотр.

Этот вывод имеет логическое обоснование. Обнаружив в ходе производства следственного действия (осмотра места происшествия, обыска,

выемки) какой-либо документ, содержащий значимые для уголовного дела сведения на бумажном носителе, например, письмо, уже полученное адресатом (потерпевшим, подозреваемым или иным лицом), или еще не отправленное им, следователь вправе его изъять и осмотреть по правилам статьи 177 УПК РФ. Для этого ему не требуется специальное судебное решение. Что же в таком случае отличает электронное сообщение от сообщения на бумажном носителе? С точки зрения уголовно-процессуального закона – ничего. Это тот же «иной документ», как его понимает законодатель (ст. 84 УПК РФ). Часть 2 статьи 84 УПК РФ гласит, что документы могут содержать сведения, зафиксированные как в письменном, так и в ином виде. К ним могут относиться фото- и видеодокументы, а также сведения, зафиксированные на ином носителе информации. Таким носителем информации может быть и электронный носитель информации. Это приводит к тому же выводу, к которому пришел и Конституционный Суд РФ: электронные сообщения на изъятых в ходе проведения следственных действий электронных носителях информации могут быть осмотрены без получения для этого специального судебного решения.

Если же рассматривать ситуацию, когда электронный носитель информации с имеющими значение для уголовного дела сведениями не находится в

¹⁰ Хайдаров А. А. О гарантиях прав граждан на тайну переписки, телефонных и иных переговоров в контексте определения Конституционного Суда Российской

Федерации от 25.01.2018 № 193-О // Вестник Университета прокуратуры Российской Федерации. 2018. № 5 (67). С. 79.

распоряжении следователя, тогда для осмотра электронных сообщений, находящихся на этом носителе, действительно потребуется решение суда. Здесь речь идет об информации,

доступа к которой у следователя нет. И получая такой доступ не от абонента, а, например, от оператора связи, он нарушает конституционное право граждан на тайну переписки.

Список литературы

1. Бикмиев Р. Г. Выемка и осмотр электронных устройств / Р. Г. Бикмиев, Р. С. Бурганов // Уголовное право. 2018. № 1. С. 125–131.
2. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / А. В. Аносов [и др.]. М.: Академия управления МВД России, 2019. Ч. 1. 208 с.
3. Долинин В. Н. Технологии собирания, исследования и использования электронно-цифровых доказательств // Технологии XXI века в юриспруденции: материалы Всероссийской научно-практической конференции (Екатеринбург, 24 мая 2019 года) / В. Н. Долинин, Ю. Р. Кабитова, П. С. Елькина; под ред. Д. В. Бахтеева. Екатеринбург: Уральский государственный юридический университет, 2019. С. 47–57.
4. Решение суда для фиксации переписки на смартфонах в ходе осмотра не нужно // Уголовный процесс. 2018. № 4. С. 7.
5. Хайдаров А. А. О гарантиях прав граждан на тайну переписки, телефонных и иных переговоров в контексте определения Конституционного Суда Российской Федерации от 25.01.2018 № 193-О // Вестник Университета прокуратуры Российской Федерации. 2018. № 5 (67). С. 77–80.

Elena V. Nikitina

PhD (Law), Associate Professor of the Department of Judicial Activities and Criminal Procedure,
Ural State Law University
(Yekaterinburg, Russian Federation)
nick2210@yandex.ru

ELECTRONIC MESSAGES AS AN OBJECT OF PROCEDURAL EXAMINATION

Abstract: The article draws attention to the absence in the criminal procedure law of a definition of such a concept as «electronic messages». Taking into account the analysis of the Federal Law of July 27, 2006 No. 149-FZ (as amended on December 30, 2020) «On Information, Information Technologies and Information Protection», it is proposed to supplement Article 5 of the RF Criminal Procedure Code with the following concepts: «electronic message» and «information and telecommunication network». The

problem of procedural examination of electronic messages from the point of view on observance of the citizens' constitutional rights is investigated. The position of the Constitutional Court of the Russian Federation in the decision of January 25, 2018 No. 189-O is given. Various interpretations of this decision, proposed in the specialized literature, are presented. The author represents her own vision of the problem, as well as the position of the Constitutional Court of the Russian Federation.

Keywords: electronic messages, information and telecommunication network, electronic media, procedural examination, court decision.

Табаков Александр Владимирович

Кандидат юридических наук, доцент кафедры судебных экспертиз, доцент,

Санкт-Петербургский государственный

архитектурно-строительный университет

(г. Санкт-Петербург, Российская Федерация)

tabakov@mail.ru

**О ФОРМАХ ФИКСАЦИИ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ НА
СОВРЕМЕННОМ ЭТАПЕ РАЗВИТИЯ КРИМИНАЛИСТИКИ**

Аннотация: В статье ставится вопрос о необходимости ревизии криминалистической теории фиксации доказательственной информации. Отмечается, что в условиях информатизации и цифровизации современного общества появляются новые типы криминалистических объектов и новые средства и способы фиксации, которые выходят за рамки традиционной концепции. Автором показано, что перечень из четырёх форм фиксации доказательственной информации уже не охватывает все возможные способы фиксации. В частности, вербальная фиксация, вопреки мнению большинства криминалистов, не может включать в себя аудиозапись. Для последней необходимо выделить отдельную форму – фоноскопическую. Также поднята проблема фиксации материальной обстановки при помощи компьютерного моделирования.

Ключевые слова: доказательственная информация, формы фиксации, аудиозапись, фоноскопия, компьютерное моделирование.

Для цитирования:

Табаков А. В. О формах фиксации доказательственной информации на современном этапе развития криминалистики // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 382–388.

В историческом плане криминалистическое учение о фиксации доказательственной информации – одно из самых «ранних», зародившихся на начальном этапе формирования криминалистики как науки. Вопросы фиксации доказательственной информации «традиционно» находятся в поле зрения криминалистов ввиду особого прикладного значения данного

элемента собирания доказательств (а криминалистика, как известно, – прикладная наука, нацеленная, прежде всего, на решение практических задач, возникающих в ходе выявления, предупреждения, расследования и раскрытия преступлений). Криминалистическое учение о фиксации доказательственной информации уже прошло длинный путь развития, начиная с разработки и систематизации практических

рекомендаций по применению технико-криминалистических средств, приёмов и методов фиксации и заканчивая рассмотрением фиксации с точки зрения философии (гносеологии) и теории информации.

Однако в контексте информатизации и цифровизации современного общества появляются новые типы криминалистических объектов и, соответственно, новые средства и способы фиксации, которые не «укладываются» в давно устоявшуюся концепцию. В этой связи возникают проблемные вопросы. Инновации требуют не только разработки соответствующих практических рекомендаций для субъектов противодействия преступности, но и теоретического осмысления в рамках криминалистического учения о фиксации доказательственной информации.

Обратимся к такому разделу рассматриваемого учения как формы фиксации доказательственной информации. По данному вопросу большинство криминалистов проявляют единодушие. В практически всех учебно-методических и научных изданиях по криминалистике, затрагивающих эту тему, выделяются четыре формы фиксации доказательственной информации: 1) вербальная (словесная); 2) графическая; 3) предметная; 4) наглядно-образная¹. К числу методов, реализующих

перечисленные формы фиксации, отмечаются: 1) при вербальной форме – протоколирование, звукозапись; 2) при графической форме – изготовление схем, планов, чертежей, рисунков; 3) при предметной форме – изъятие предмета в натуре и его консервация, изготовление материальных моделей (реконструкция), в том числе макетирование, изготовление слепков и оттисков; 4) при наглядно-образной форме – фотографирование (в видимых и невидимых лучах), кино- и видеосъёмка². Отмечается, что возможны комбинации форм, методов и технических приёмов фиксации доказательственной информации.

Первый взгляд на представленную выше совокупность форм фиксации доказательственной информации приводит к предварительному выводу о том, что в их названиях заключены средства и способы фиксации. При вербальной форме для целей фиксации и в качестве средств фиксации используются слова, точнее, тексты; при графической форме – графические отображения; при предметной форме – предметы, то есть материальные объекты, включая модели; при наглядно-образной форме – фотоизображения и иные наглядные образы.

Но давайте более внимательно рассмотрим первую форму фиксации доказательственной информации – вербальную. Эта форма исторически

¹ См.: Белкин Р. С. Курс криминалистики. В 3 т. Т. 2: Частные криминалистические теории М.: Юристъ, 1997. С. 125; Криминалистика: Учебник / отв. ред. Н. П.

Яблоков. 3-е изд., перераб. и доп. М.: Юристъ, 2005. С. 58 и мн. др.

² См.: Белкин Р. С. Курс криминалистики. В 3 т. Т. 2: Частные криминалистические теории М.: Юристъ, 1997. С. 125.

является самой старой и сравнительно простой, она не требует специальных технико-криминалистических средств, что делает её практически общедоступной³. Та интерпретация данной формы фиксации, которая представлена в криминалистической литературе, вызывает у нас сомнения, хотя она (интерпретация) является, так сказать, «традиционной».

Р. С. Белкин и множество других учёных связывают с вербальной, то есть словесной формой фиксации различные виды описания (протоколирование, словесный портрет) и звукозапись. Однако, если исходить из приведённого выше постулата, согласно которому сущность и специфика формы фиксации выражается в средствах и способах фиксации, и, соответственно, термин, означающий ту или иную форму, отражает эти средства и способы, то нужно сделать вывод: описание (в частности, протоколирование) и звукозапись не являются и не могут являться примерами одной и той же формы фиксации!

Поясним нашу мысль. Вербальная форма фиксации доказательственной информации означает то, что фиксация осуществляется словами, при помощи слов. Протоколирование и иные способы фиксации при помощи

языковых единиц под эту характеристику вполне подпадают. При этом протоколирование может применяться для фиксации как речевой информации (протокол допроса, протокол очной ставки и др.) – в этом случае происходит фиксация слов (устной речи) с помощью слов (письменной речи), так и для фиксации информации, не выражаемой речью, например, информации, содержащейся в вещной обстановке (протокол осмотра места происшествия, протокол обыска и др.)⁴. В любом случае эти способы фиксации основаны на использовании языковых средств запечатления. Но звукозапись – нет! – она не относится к фиксации, осуществляемой словесным способом. Как видно из представленных в криминалистической литературе примеров вербальной фиксации и пояснений по её применению, при помощи звукозаписи фиксируются слова (речь допрашиваемого и т. п.), но не осуществляется фиксация словами, то есть *при помощи слов*.

Звукозапись – это процесс фиксации звуковых сигналов (сигналов звукового частотного диапазона, или аудиосигналов) на носитель (материальный объект для фиксации, хранения и считывания сигналов) с возможностью последующего воспроизведения;

³ См Белкин Р. С. Курс криминалистики. В 3 т. Т. 2: Частные криминалистические теории М.: Юристъ, 1997. С. 137.

⁴ При протоколировании упомянутых следственных действий, связанных с восприятием визуальной информации (осмотр места происшествия, обыск), объектом вербальной фиксации тоже может быть словесно выраженная информация. Но

в данных случаях это будет не устная речь, как, например, при допросе, а письменная речь (например, надписи на каких-либо криминалистических объектах), которая фиксируется при помощи всё той же письменной речи в протоколе. Перекодировка информации не происходит, только осуществляется замена носителя информации.

результатом звукозаписи является фонограмма⁵. Совокупностью звуковых сигналов может быть, конечно, и устная речь человека (речевой сигнал⁶). Однако речь в данном случае является не средством фиксации, а её объектом. Средствами же фиксации являются технические устройства, обеспечивающие перекодировку акустических сигналов в аналоговые или цифровые сигналы, создание фонограммы с возможностью последующего воспроизведения (считывания с носителя звуковых сигналов и преобразование их в заданный вид)⁷. Следовательно, звукозапись не относится к вербальной форме фиксации, так как фиксация осуществляется не при помощи языковых средств.

В правильности этого хода мыслей убеждаешься ещё больше, когда обращаешь внимание на тот факт, что аудиосигналы, которые фиксируются посредством звукозаписи, могут вообще не являться речевыми сигналами (не

содержать звучащую речь); это могут быть и иные звуки (шумы и пр.). И кстати, звуки, не являющиеся устной речью, нередко выступают в качестве объектов криминалистического исследования, например, в ходе инженерно-технических (фоноскопических, автотехнических и др.) экспертиз. В случае фиксации при помощи звукозаписи таких звуков, которые не образуют устную речь человека, слова в принципе не фигурируют – ни в качестве объекта фиксации, ни в качестве её средства. И при чём тут, спрашивается, вербальная фиксация?! Очевидно, ни при чём – мы не видим и не слышим ни одного слова.

Полагаем, что звукозапись отнесена к вербальной форме фиксации потому, в большинстве случаев она действительно используется для фиксации слов (устной речи); в ходе предварительного расследования звукозапись чаще всего используется при производстве таких следственных действий как допрос, очная ставка,

⁵ См.: ГОСТ Р 58332-2018. Судебная экспертиза фонограмм. Термины и определения: национальный стандарт Российской Федерации: утверждён и введён в Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2018 года № 1158-ст: дата введения: 2019–01–06 // Электронный фонд правовых и нормативно-технических документов. URL: <https://docs.cntd.ru/document/1200161961> (дата обращения: 15.05.2021).

⁶ ГОСТ Р 58332-2018. Судебная экспертиза фонограмм. Термины и определения: национальный стандарт Российской Федерации: утверждён и введён в Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря

2018 года № 1158-ст: дата введения: 2019–01–06 // Электронный фонд правовых и нормативно-технических документов. URL: <https://docs.cntd.ru/document/1200161961> (дата обращения: 15.05.2021).

⁷ Запись аналоговой фонограммы включает в себя преобразование акустических колебаний в аналоговый сигнал и его фиксацию на носитель. Запись цифровой фонограммы включает в себя преобразование акустических колебаний в аналоговый сигнал, аналого-цифровое преобразование сигнала, кодирование сигнала в звуковые данные и их фиксацию на носитель (см.: ГОСТ Р 58332-2018. Судебная экспертиза фонограмм. Термины и определения).

контроль и запись переговоров⁸. Но, во-первых, как показано ранее, звукозапись может вообще не оперировать словами ни в качестве объекта, ни в качестве средства фиксации – основания для её отнесения к вербальной форме фиксации в таких случаях в принципе отсутствуют. Во-вторых, толкование вербальной формы фиксации как формы, связанной с запечатлением либо слов, либо при помощи слов, представляется некорректным с точки зрения формальной логики: здесь происходит подмена понятий и деление по разным основаниям – типичные логические ошибки.

Итак, звукозапись любых – как речевых, так и неречевых – звуковых сигналов однозначно нельзя отнести к таким формам фиксации как графическая, предметная, наглядно-образная: в этом нет сомнений и по этому поводу нет споров среди криминалистов. В качестве графической формы фиксации можно рассматривать лишь графическое изображение амплитудно-частотно-временных характеристик звука, но это уже – не звукозапись, ибо не создаётся фонограмма. Взятую нами в качестве яркого примера звукозапись неречевых аудиосигналов также невозможно отнести ни к одной из четырёх означенных форм фиксации доказательственной информации. Выше мы объяснили, что такая разновидность звукозаписи не может считаться вербальной формой фиксации: объект фиксации (звук) не

является речью и в ходе фиксации не осуществляется вербализация. Наконец, единственный вариант, когда звукозапись связана с языком (звучащей речью), – это вариант звукозаписи устной речи – тоже некорректно относить к вербальной форме фиксации, если деление форм фиксации основывать на признаке применяемых для запечатления средств и методов.

Изложенное подводит к «крамольному» выводу: практически никем не оспариваемый перечень форм фиксации доказательственной информации, включающий четыре формы, является неправильным, поскольку он трактуется как исчерпывающий, но не охватывает некоторые используемые на практике методы фиксации. Распространённую в криминалистических источниках позицию, согласно которой звукозапись представляет собой вербальную форму фиксации, следует признать некорректной с формально-логической точки зрения, ибо наблюдается деление по разным основаниям: формы фиксации выделяются в зависимости от применяемых для запечатления средств и методов, однако для звукозаписи «делается исключение»: она «примыкает» к вербальной форме фиксации по другому основанию, а именно – по признаку отнесения объекта фиксации к словесному материалу (устной речи).

Полагаем, что звукозапись – это пример проявления иной, отличной от

⁸ Если при проведении допроса и очной ставки звукозапись факультативна (часть 4 статьи 189 УПК РФ), то контроль и запись переговоров – это следственное действие,

прямо ориентированное на производство звукозаписи и получение в результате фонограмм (статья 186 УПК РФ).

четырёх известных форм фиксации доказательственной информации. Как отмечалось, в процессе звукозаписи создаётся фонограмма (от греч. φωνή – «звук» + γράμμα – «запись») – звуковые сигналы, содержащиеся на аналоговом или цифровом носителе, или записанные в определённом файле. В этой связи выносим на обсуждение учёного сообщества вопрос о возможности и целесообразности расширения списка форм фиксации путём включения в него пятой формы – фонографической.

Думается, что предлагаемое нами дополнение снимет противоречия между теорией и практикой, «расставит вещи по своим местам». Звукозаписи будет отведено своё «законное» место. А весьма часто применяемая в правоохранительной деятельности видеозвукозапись, результатом которой является видеофонограмма (записанные на носителе аудио- и видеосигналы)⁹, будет рассматриваться как сочетание двух форм фиксации – наглядно-образной и фонографической.

Мы осознаём, что наше предложение, возможно, излишне «смелое». Но ведь для исследователя не должно быть предустановленных догм и непререкаемых авторитетов, не так ли? К любым научным достижениям нужно относиться критично, в том числе (и прежде всего) к своим собственным.

Криминалистическое учение о фиксации доказательственной информации, хоть и достаточно «зрелое», не должно быть в этом плане исключением. Как нам видится, сложились предпосылки к ревизии данной теории. Помимо обозначенной в настоящей статье проблемы, связанной с отсутствием для звукозаписи места в перечне форм фиксации, имеются и иные, не менее актуальные проблемы. Так, аналогичный по существу вопрос можно поставить в отношении такого способа фиксации, как создание цифровой модели материального объекта (вещной обстановки и др.) на основании данных, получаемых, в частности, путём лазерного сканирования местности. Возможность его отнесения к предметной форме фиксации (моделирование, как известно, относят именно к этой форме) вызывает у нас некоторые сомнения, поскольку фиксация осуществляется не «предметно» в «классическом» варианте интерпретации указанной формы. С другой стороны, мы понимаем, что этот вопрос дискуссионный, ведь цифровая информация на том или ином носителе тоже имеет материальную природу¹⁰. В контексте тотальной цифровизации цифровую модель, представляющую собой компьютерную информацию на том или ином материальном носителе, с определёнными оговорками можно

⁹ См.: ГОСТ Р 58332-2018. Судебная экспертиза фонограмм. Термины и определения.

¹⁰ См.: Россинская Е. Р., Семикаленова А. И. Основы учения о криминалистическом исследовании компьютерных средств и

систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник СПбГУ. Право. 2020. Т. 11, вып. 3. С. 745–759.

назвать «предметом» и отнести, стало быть, к проявлению предметной формы фиксации доказательственной информации. При таком подходе данная форма, соответственно, будет интерпретироваться более широко, объём понятия «предметная форма фиксации» будет увеличен. Эти вопросы также нуждаются в обсуждении.

Ясно одно: в настоящее время, в условиях стремительного научно-технического прогресса криминалисты сталкиваются с новыми вызовами, но вместе с тем им открываются и новые возможности. В этих условиях некоторые, казавшиеся незыблемыми устои криминалистики требуют переосмысления.

Список литературы

1. Белкин Р. С. Курс криминалистики. В 3 т. Т. 2: Частные криминалистические теории. М.: Юристъ, 1997. – 464 с.
2. Криминалистика: Учебник / отв. ред. Н. П. Яблоков. 3-е изд., перераб. и доп. М.: Юристъ, 2005. 781 с.
3. Россинская Е. Р. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова // Вестник СПбГУ. Право. 2020. Т. 11, вып. 3. С. 745–759.

Alexander V. Tabakov

PhD (Law), Associate Professor of Forensic Examinations Department,
Associate Professor,
Saint Petersburg State University of Architecture and Civil Engineering
(Saint Petersburg, Russian Federation)
tabakov@mail.ru

ON THE FORMS OF FIXING EVIDENTIARY INFORMATION AT THE PRESENT STAGE OF DEVELOPMENT OF FORENSIC SCIENCE

Abstract: The article raises the question of the need to revise the forensic theory of evidence fixing. It is noted that in the conditions of informatization and digitalization of modern society, new types of forensic objects and new means and methods of fixation appear that go beyond the traditional concept. The author shows that the list of four forms of fixing evidential information no longer covers all possible ways of fixing. In particular, verbal fixation, contrary to the opinion of most forensic scientists, cannot include audio recording. For it, it is necessary to select a separate form – phonoscopic fixation. The problem of fixing the material situation with the help of computer modeling was also raised.

Keywords: evidentiary information, fixation forms, audio recording, phonoscopy, computer modelling.

УДК 343.14

Архипова Екатерина Александровна

Кандидат юридических наук, старший научный сотрудник отдела научного обеспечения международного сотрудничества прокуратуры и сравнительного правоведения НИИ,

Университет прокуратуры Российской Федерации

(г. Москва, Российская Федерация)

e.arkhipova@bk.ru

ПРАВОВОЙ СТАТУС И ПРОЦЕДУРА ПРИЗНАНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В КАЧЕСТВЕ ДОКАЗАТЕЛЬСТВ В УГОЛОВНОМ ПРОЦЕССЕ ИНОСТРАННЫХ ГОСУДАРСТВ

Аннотация: На основе анализа правовой регламентации использования электронных доказательств в уголовном процессе иностранных государств автором сделан вывод о необходимости закрепления в УПК РФ четких и однозначных оснований и правил собирания доказательств путем использования современных электронных технологий.

Ключевые слова: электронные доказательства, киберпреступность, уголовный процесс, оказание правовой помощи по уголовным делам.

Для цитирования:

Архипова Е. А. Правовой статус и процедура признания электронных документов в качестве доказательств в уголовном процессе иностранных государств // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 389–400.

В современном мире электронная информация является повсеместной и формируется в возрастающих объемах, разновидностях и скоростях. Электронная информация может быть использована как во благо человека и общества (электронная навигация, электронные медицинские консультации и карты, электронный банкинг и др.), так и в преступных целях.

Современные технологии стали распространенным средством совершения преступлений и надежным носителем информации,

электронные следы которой правоохранительные органы и суды используют для восстановления и фиксации картины произошедшего.

Новые технологии позволили совершать не только новые виды преступлений, но и оказали значительное влияние на то, насколько успешно можно раскрывать и расследовать преступления. Поскольку преступления все чаще совершаются в Интернете, то сбор и процессуальное закрепление электронных доказательств имеют важное значение для осуществления

эффективного и законного уголовного преследования.

Глобализация преступности вызывает необходимость совершенствования методов борьбы с ней и тесного взаимодействия компетентных органов государств, в том числе в сфере оказания взаимной правовой помощи по уголовным делам. Анализ соответствующей практики показывает возрастающую потребность применения новых способов и средств собирания доказательств, особенно с использованием новых технологий.

Именно поэтому в целях эффективного раскрытия преступлений и осуществления уголовного преследования лиц, их совершивших, государства должны оперативно адаптироваться к быстрому развитию и использованию технологий, в частности, в работе с электронными доказательствами.

Правовой статус и процедура признания электронных документов в качестве доказательств в уголовном судопроизводстве зависит от принадлежности государства к той или иной правовой семье.

Для большинства европейских стран характерна высокая проработанность правовых понятий, терминов и, соответственно, классификации средств доказывания. В то же время англо-саксонская правовая семья характеризуется

большой ролью судебного прецедента и прикладной юридической доктриной. Здесь вопрос о том, являются ли «электронные доказательства» самостоятельным видом доказательств, не имеет существенного значения и юридические понятия не так важны.

В странах Европейского Союза имеются разнообразные подходы в отношении электронных доказательств по уголовным делам. В связи с этим была принята директива, обязывающая назначать своего законного представителя в Союзе для получения, соблюдения и обеспечения исполнения решений, направленных на сбор доказательств компетентными национальными органами в рамках уголовного судопроизводства.

В 2019 г. Комитетом министров Совета Европы приняты Руководящие принципы по электронным доказательствам в гражданских и административных производствах, которые актуальны и для использования в уголовном процессе¹.

В большинстве европейских стран, допустимость электронных доказательств в ходе предварительного расследования и судебного разбирательства уголовного дела, как правило, регулируется общими положениями уголовно-процессуального законодательства о традиционных доказательствах².

¹ Electronic evidence in civil and administrative proceedings: guidelines adopted by the Committee of Ministers on 30 Jan. 2019, at the 1335th meeting of the Ministers' Deputies and Explanatory Memorandum // Committee of Ministers of the Council of Europe: official site. URL: <https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory->

[memorandum/1680968ab5](https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5) (accessed: 17.05.2021).

² Научное обеспечение деятельности органов прокуратуры в 2020 году: сб. науч. докл. Вып. 9 / под общ. ред. О. С. Капинус; Ун-т прокуратуры Рос. Федерации. М., 2021. С. 225.

В уголовно-процессуальном законодательстве ФРГ среди процессуальных действий, направленных на получение доказательств об обстоятельствах совершенного общественно опасного деяния, предусмотрены контроль телекоммуникации, прослушивание и запись высказываний, сделанных непублично, применение технических средств и др.

В УПК Швейцарии предусмотрено, что органы власти должны использовать каждое допустимое доказательство, которое основано на положениях научного знания и опыте и может служить для установления истины. Швейцарское законодательство не содержит абсолютных ограничений видов доказательств, которые могут быть представлены в суде. Поэтому органы власти могут использовать новые доказательства в результате научного прогресса, даже если они прямо не закреплены в процессуальном праве.

В Законе об уголовном процессе Испании предусмотрены такие электронные доказательства как средства воспроизведения слов, звуков и изображения, а также инструменты, разрешающие или воспроизводящие слова, цифры и математические операции, выполняемые для целей бухгалтерского учета или других целей, относящихся к судебному разбирательству.

Согласно Уголовному кодексу Италии под электронным документом понимается любой компьютерный инструмент, который содержит информацию с доказательственной значимостью или любым указанным

программным обеспечением для обработки такой информации.

В Уголовно-процессуальном законе Австралии 2007 г. под доказательственным материалом понимают вещь, имеющую отношение к преступлению, включая такую вещь в электронной форме. Стоит отметить, что австралийские законодатели также нормативно закрепили возможность исполнения запросов иностранных государств о получении компьютерной информации (Закон о взаимной правовой помощи по уголовным делам 1987 г.).

Допустимость в качестве доказательств цифровых документов предусмотрена по законодательству Бельгии, Голландии, Португалии, Румынии, Финляндии и ряда других стран.

Таким образом, в законодательстве стран Европы отсутствуют конкретное определение электронных доказательств по уголовным делам, а также правила их допустимости в ходе расследования и судебного разбирательства уголовного дела. Как правило, электронные документы сопоставляются с бумажными документами для придания им ценности в качестве доказательств.

В Великобритании сотрудник полиции, осуществляющий расследование преступления, должен иметь возможность фиксировать доказательства в цифровом виде на месте преступления (в частности, показания потерпевших и свидетелей), принимать заявления и загружать информацию по делу с помощью мобильных устройств. Впоследствии данная цифровая информация

передается в Королевскую службу обвинения для принятия решения о предъявлении подозреваемому лицу обвинения. Собранные по делу электронные доказательства без их дублирования на бумажном носителе в дальнейшем исследуются в суде и используются им для принятия итогового решения по уголовному делу.

В Шотландии также предполагается полный отказ от бумажного формата уголовного дела и использование Системы хранения цифровых доказательств. Данная Система предназначена для работы с различного вида доказательствами, получения к ним доступа со стороны уполномоченных на то участников уголовного судопроизводства.

Сотрудники полиции Англии, Уэльса и Северной Ирландии в своей деятельности при расследовании преступлений опираются на Руководство по работе с цифровыми доказательствами. Данным документом

устанавливаются определенные требования к лицам, участвующим в собирании электронных доказательств, а также в идентификации цифровой информации, необходимой для расследования преступлений.

Основными принципами работы с цифровыми доказательствами по делу являются: неизменяемость полученных данных, которые впоследствии могут быть использованы в суде; компетентность должностных лиц относительно изъятых доказательств, последствий и

содержания своих действий; ведение записей всех процессов, применяемых к цифровым доказательствам; ответственность должностных лиц, осуществляющих расследование, за реализацию принципов работы с цифровыми доказательствами.

В США под электронными (цифровыми) доказательствами понимается любая информация, которая хранится или передается в цифровой форме и которую сторона уголовного процесса может использовать в качестве доказательства в судебном разбирательстве³.

Закон США, регулирующий электронные доказательства в уголовных расследованиях, имеет два основных источника: Четвертая поправка к Конституции США и статутные законы о неприкосновенности частной жизни, кодифицированные в 18 U. S. C. §§ 2510–22, 18 U. S. C. §§ 270112 и 18 U. S. C. §§ 3121–27.

В США процедуры доказывания с использованием цифровых доказательств по уголовному делу более подробно регламентируются в Руководстве по поиску и собиранию электронных доказательств. В соответствии с данным нормативным актом электронные доказательства классифицируются на прямые и косвенные.

К прямым доказательствам относятся те, которые сгенерированы ЭВМ без участия человека и подразделяются на две категории: 1)

³ См.: Casey E. Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet. 3rd ed. Baltimore, 2011. P. 7.

записи, созданные компьютером; 2) записи, хранящиеся в памяти ЭВМ.

Косвенные доказательства содержат результат деятельности человека (письма, памятки, документы бухгалтерского учета и т. д., созданные людьми), к ним применяются правила исследования косвенных доказательств.

С учетом происхождения выделяются две группы компьютерных доказательств: 1) результаты деятельности человека, хранящиеся на электронном носителе (жестком диске, флоппи-диске, компакт-диске, стримере) и содержащие информацию, внесенную пользователем; 2) доказательства, созданные компьютером в соответствии с заложенной программой и представляющие собой результат обработки тех или иных начальных данных.

Внедрение электронного документооборота в информационно-документационные процессы не обошло стороной и государств – участников СНГ. Работа над созданием законодательных и других нормативных правовых актов, регулирующих использование электронного документа и электронной цифровой подписи и наделяющих их юридической силой, велась как внутри государств, так и в рамках Содружества.

В частности, на шестнадцатом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ был принят Модельный закон «Об электронной цифровой подписи» (постановление № 16-10 от 9 декабря 2000 года), который представляет

собой свод унифицированных правил и процедур в рамках СНГ, принятый всеми участниками. Наличие такого закона обеспечивает юридически закрепленный обмен электронными документами в рамках СНГ.

Рассмотрение электронных сведений в форме электронного документа является позитивным моментом в реформировании доказательственного права. Так, в Рекомендациях по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях для государств – участников СНГ от 29 ноября 2013 г. закреплено, что особенностью современного терроризма является то, что террористами широко используется информационно-техническое воздействие на отдельные элементы информационно-телекоммуникационной инфраструктуры государств с целью нанесения им ущерба, а также их подавления и уничтожения.

Анализ нормативных правовых актов государств – участников СНГ показал, что уголовно-процессуальным законодательством Азербайджанской Республики электронная информация определена в качестве электронного документа, электронный носитель информации не составляет самостоятельного вида доказательств. В Уголовно-процессуальном кодексе Республики Армения отсутствуют специальные нормы, определяющие порядок хранения и оценки электронной информации.

В ст. 122 УПК Республики Армения в качестве доказательств электронная информация и машинные носители информации отнесены к другим документам.

В соответствии с УПК Республики Армения электронная информация и электронные носители информации могут быть получены при производстве осмотра, в ходе которого может использоваться фото-, кино-, видеосъемка и иная форма фиксации (ст. 218). В ходе обыска (ст. 225, 228), выемки (ст. 226), личного обыска (ст. 229), контроля корреспонденции, почтовых, телеграфных и иных сообщений (ст. 239), осмотра и выемки корреспонденции (ст. 240), прослушивания телефонных переговоров (ст. 241) могут быть использованы технические средства.

УПК Республики Армения устанавливает определенный порядок сбора электронной корреспонденции. К корреспонденции, на которую может быть наложен арест, в ч. 3 ст. 239 УПК отнесены сообщения по телефаксу и электронной почте.

Следственные действия, предусмотренные статьями 239, 240, 241 УПК производятся на основании решения суда, участие в них специалиста не является обязательным. Специальных требований к выемке, хранению электронной информации и электронных носителей информации в законе не установлено.

Анализируя правовое регулирование использования электронной информации и электронных носителей информации в уголовном судопроизводстве

Республики Армения можно выделить следующие особенности: регламентирован порядок ареста электронной корреспонденции, допустимо производство копирования такой информации; определен правовой статус законного владельца изъятого электронного документа; установлен порядок возбуждения уголовного дела на основании электронного сообщения юридического лица; в законе не закреплен специальный порядок сбора электронных носителей информации.

Уголовно-процессуальный кодекс Республики Беларусь (далее по тексту – УПК РБ) четко разграничивает доказательства (фактические данные) и источники доказательств. В качестве критериев оценки источников доказательств УПК РБ выделяет относимость, допустимость, достоверность и достаточность, отмечая в ч. 3 ст. 105 УПК РБ, что допустимость распространяется именно на источники доказательств. В качестве доказательства законодатель определяет «любые фактические данные, полученные в предусмотренном законом порядке» (ч. 1 ст. 88 УПК РБ).

Источниками доказательств (ч. 2 ст. 88 УПК РБ) являются показания подозреваемого, обвиняемого, потерпевшего, свидетеля, заключение эксперта, в том числе документы и другие носители информации, полученные в порядке, предусмотренном УПК РБ. Закон не содержит определения доказывания, а закрепляет лишь элементы процесса доказывания, определяя его цели.

В соответствии со ст. 103 УПК РБ собрание доказательств осуществляется путем проведения следственных действий, представления имеющих значение для дела предметов и документов, а также производства проверок соответствующими органами и должностными лицами по требованию органа уголовного преследования или суда.

Кроме того, ст. 224.1 УПК РБ «Проведение допроса, очной ставки, предъявление для опознания с использованием систем видеоконференцсвязи» и ст. 343.1 УПК РБ «Проведение допроса, опознания с использованием систем видеоконференцсвязи» предусмотрена возможность дистанционного сбора удаленных данных на этапе предварительного расследования и в ходе судебного следствия путем использования системы видеоконференцсвязи.

На основании изложенного можно сделать вывод, что электронная информация и электронные носители информации не выделены в качестве самостоятельного источника доказательств, соответственно, в отношении данной информации не установлен особый порядок сбора, хранения, представления и оценки. Однако представляет интерес нормативное закрепление в УПК РБ возможности получения доказательственной информации путем проведения очной ставки и предъявления для опознания в режиме видеоконференцсвязи.

Глава 15 Уголовно-процессуального кодекса Республики Казахстан (далее по тексту – УПК РК)

закрепляет следующие виды доказательств: показания подозреваемого, потерпевшего, свидетеля; заключение и показания эксперта; заключение и показания специалиста; вещественные доказательства; протоколы процессуальных действий; документы. Кодекс не содержит определения документа, однако в соответствии со ст. 120 УПК РК к документам, которые могут быть представлены в качестве источника доказательств, отнесены сведения, зафиксированные в письменной форме или иным способом (компьютерная информация, фото- и киносъемка, видео- и звукозапись).

В соответствии со ст. 123 УПК РК фактические данные могут быть использованы в качестве доказательств лишь после их фиксации в протоколах процессуальных действий. Для закрепления доказательств, помимо прочего, могут применяться фотосъемка, звукозапись, киносъемка и видеозапись. Полученные фотоснимки, видеозаписи, фонограммы и кинофильмы прилагаются к протоколу.

Ст. 126 УПК РК регулирует применение научно-технических средств в процессе доказывания. На основании этой нормы, например, доказательством может выступать видеозапись с видеорегистратора, с камер видеонаблюдения.

Также УПК РК предусматривает институт депонирования показаний и возможность дистанционного допроса. Согласно ст. 217 УПК РК участники судопроизводства вправе заявить ходатайство о проведении

допроса следственным судьей, в случае если имеются основания полагать, что более поздний допрос может оказаться невозможным. Осуществляющее досудебное расследование лицо вправе направить заявление прокурору о направлении следственному судье ходатайства о депонировании показаний. Кроме того, в ст. 213 УПК РК предусмотрен дистанционный допрос потерпевшего или свидетеля, который может быть произведен с использованием научно-технических средств в режиме видеосвязи.

Уголовно-процессуальный кодекс Кыргызской Республики (далее по тексту – УПК КР) признает доказательствами любые фактические данные, на основе которых в порядке, определенном в законе, следователь, прокурор, суд устанавливают наличие или отсутствие деяния, предусмотренного Уголовным Кодексом, совершение или не совершение этого деяния подозреваемым, обвиняемым, подсудимым и виновность или невиновность подсудимого, а также иные обстоятельства, имеющие значение для правильного разрешения дела. Материалы фото- и киносъемки, звуко- и видеозаписи, признанные доказательством по делу, определяются в качестве иных документов.

В УПК КР доказательства определены как полученные в установленном законом порядке сведения, на основе которых орган дознания, следователь, прокурор, суд определяют наличие или отсутствие обстоятельств, имеющих значение для дела (ст. 82 УПК КР).

К источникам доказательств, помимо закрепленных в действующем уголовно-процессуальном законе, относятся показания эксперта и специалиста. Согласно ч. 3 ст. 91 электронный документ признается доказательством, равным по своей значимости письменным доказательствам, и имеет одинаковую юридическую силу с документом, воспроизведенным на бумажном носителе.

В отношении электронных носителей информации установлен особый порядок хранения и сбора (п. 8 ч. 2 ст. 89, ч. 16 ст. 205 УПК КР). По ходатайству владельца изымаемых носителей производится копирование содержащихся на нем данных.

Особый интерес представляет ч. 2 ст. 193 УПК КР, согласно которой с использованием обязательной аудио- и видеофиксации подлежат проведение допроса несовершеннолетних; слепых; неграмотных; малограмотных, которые не в состоянии прочесть записи своих показаний в протоколе допроса; лиц, допрашиваемых через переводчика, обвиняемых по делам об особо тяжких преступлениях; лиц, нуждающихся в исследовании экспертами-психиатрами; при даче признательных показаний подозреваемыми, обвиняемыми о совершении ими преступлений.

Кроме того, предусматривается проведение допроса с использованием технических средств в режиме видеосвязи (дистанционный допрос), в ходе которого предъявляются требования к качеству изображения, звука, а также к обеспечению информационной безопасности, (ст.

194 УПК КР), предъявления для опознания (ст. 202 УПК КР) и производство допроса судом с применением видеоконференцсвязи (ст. 280 УПК КР).

Уголовно-процессуальный кодекс Республики Молдова (далее по тексту – УПК РМ) определяет доказательства как полученные в определенном законом порядке фактические данные, на основе которых устанавливаются наличие или отсутствие признаков преступления, личность совершившего преступление, виновность или невиновность обвиняемого, а также иные обстоятельства, имеющие значение для правильного разрешения дела (ст. 93 УПК РМ).

Аудио- и видеозаписи, фотографии, средства электронно-технического, магнетического, оптического контроля и другие носители электронно-технической информации, полученные в соответствии с требованиями законодательства, являются средствами доказывания, если содержат сведения или веские признаки подготовки или совершения преступления и если их содержание способствует установлению истины по делу (ст. 164 УПК РМ).

В УПК Республики Молдова регламентирован порядок проведения электронного обыска и изъятия электронной информации (ст. 130-1 УПК РМ), мониторинга онлайн-активности пользователей сети Интернет на основании решения суда (ст. 132-11 УПК РМ).

Уголовно-процессуальный кодекс Республики Таджикистан

определяет доказательства как фактические сведения, на основе которых суд, следователь, дознаватель, прокурор, устанавливая наличие либо отсутствие общественно опасного деяния, доказанности или недоказанности совершения этого деяния и другие обстоятельства, которые могут иметь значение для правильного разрешения дела (ч. 1 ст. 72 УПК Республики Таджикистан).

Анализ уголовно-процессуального законодательства Республики Таджикистан позволяет сделать вывод о том, что закон относит к документам электронные источники информации, однако правил к их применению не содержит.

Согласно ст. 131 УПК Туркменистана в качестве доказательств служат имеющие практическое значение для дела фактические данные следственных, судебных действий, зафиксированные протоколами. Эти сведения могут быть зафиксированы как в письменной, так и в иной форме (аудио- и видеозапись, запись на носителях компьютерной информации).

В соответствии с ч. 1 ст. 125 УПК Туркменистана доказательства могут быть исключены в случае нарушений, которые способны повлиять на достоверность полученных доказательств. Указанное правило об исключении доказательств не может быть применено к вещественным доказательствам, полученным в результате незаконного прослушивания, незаконного обыска или других явно неконституционных действий сотрудников, так как

вещественные доказательства по сути своей достоверны.

Большой интерес среди следственный действий, закрепленных в УПК Туркменистана, представляют «Наложение ареста на корреспонденцию» (ст. 281 УПК); «Перехват сообщений» (ст. 282 УПК); и «Прослушивание и звукозаписи телефонных и иных переговоров» (ст. 283, 284 УПК). Указанные следственные действия производятся на основании постановления дознавателя или следователя, санкционированного прокурором.

Уголовно-процессуальный кодекс Республики Узбекистан (далее по тексту – УПК РУ) в качестве доказательств по уголовному делу определяет любые фактические данные, на основе которых в установленном законом порядке орган дознания, следователи и суд устанавливают наличие либо отсутствие общественно опасного деяния, виновности лица, совершившего это деяние, а также иные обстоятельства, имеющие значения для правильного разрешения дела.

К материалам, на котором выполнена документальная запись, относятся бумага, фотобумага, видео- и киноплёнка, аудиолента и т. п. Фиксация сведений на них может быть осуществлена при помощи букв, цифр, стенографических, телеграфных и иных знаков, изображений, схем и т. д. Особо значимая информация может фиксироваться при помощи различных технических устройств и

аппаратов (кино- и видеокамерой, магнитофоном и т. п.). После проверки и оценки доказательствами могут быть признаны материалы оперативно-розыскной деятельности (ст. 81 УПК РУ).

Специальных требований к сбору, хранению и оценке электронных носителей информации и электронной информации уголовно-процессуальное законодательство Республики Узбекистан не содержит.

Таким образом, государствами – участниками СНГ выработано единое понимание содержания доказательств, несмотря на отсутствие единой закрепленной в законе дифференциации (большинство УПК государств – участников СНГ определяют в качестве доказательств фактические данные). Электронная информация не выделена в качестве самостоятельного источника доказательства и, как правило, отнесена к иным документам. Электронные носители информации не определены в качестве самостоятельного вида доказательств и рассматриваются в качестве вещественного доказательства⁴.

Зарубежный опыт правовой регламентации и процедуры признания электронных документов в качестве доказательств в уголовном процессе важен и интересен для российских правоприменителей.

Новизна проблемы собирания электронных доказательств по уголовным делам заключается в разработке и создании быстрых и эффективных механизмов их

⁴ См.: Научное обеспечение деятельности органов прокуратуры в 2020 году: сб. науч. докл. Вып. 9 / под общ. ред. О. С. Капинус;

Ун-т прокуратуры Рос. Федерации. М., 2021. С. 257.

получения на территории России и зарубежных стран в порядке оказания правовой помощи.

Анализ нормативных положений УПК РФ в части собирания и использования электронных носителей информации дает основание сделать общий вывод о том, что уголовно-процессуальный закон признает, что цифровые технологии видоизменяют существующие общественные отношения, оказывают существенное влияние на юридическую сторону деятельности участников уголовного судопроизводства, поэтому их особенности и возможности должны быть учтены в УПК РФ и регламентированы в соответствующих нормах о доказательствах и доказывании при производстве по уголовным делам.

Сбор электронных доказательств на территории иностранного государства по запросам российской стороны в значительной степени зависит от внутреннего законодательства

Российской Федерации. В отсутствие единообразной правовой регламентации данного вопроса это может повлечь недопустимость доказательств, вызванную различиями в процедурных правилах, а также в порядке регулирования защиты данных. Вариативность внутренних нормативных правил может привести к проблемам допустимости электронных доказательств на практике и затруднить международное сотрудничество, поскольку электронные данные, необходимые для расследования, не сохраняются.

Закрепление в УПК РФ четких и однозначных оснований и правил собирания доказательств путем использования современных электронных технологий будет способствовать соблюдению разумных сроков производства следственных и иных процессуальных действий по установлению обстоятельств, подлежащих доказыванию по уголовным делам.

Список литературы

1. Мороз Н. О. Актуальные вопросы международного сотрудничества в борьбе с преступностью в сфере высоких технологий в рамках СНГ // Международное уголовное право и международная юстиция. 2016. № 3. С. 12–14.
2. Научное обеспечение деятельности органов прокуратуры в 2020 году: сб. науч. докл. Вып. 9 / под общ. ред. О. С. Капинус; Ун-т прокуратуры Рос. Федерации. М., 2021.
3. Основы теории электронных доказательств: монография / под ред. д-ра юрид. наук С. В. Зуева. М.: Юрлитинформ, 2019.
4. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet. 3rd ed. Baltimore, 2011.

Ekaterina A. Arkhipova

PhD (Law), Senior Researcher of the Research Institute,
University of the prosecutor's office of the Russian Federation
(Moscow, Russian Federation)
e.arkhipova@bk.ru

LEGAL STATUS AND PROCEDURE FOR RECOGNIZING ELECTRONIC DOCUMENTS AS EVIDENCE IN CRIMINAL PROCEEDINGS OF FOREIGN STATES

Abstract: Based on the analysis of the legal regulation of the use of electronic evidence in the criminal process of foreign states, the author concludes that it is necessary to consolidate clear and unambiguous grounds and rules for collecting evidence by using modern electronic technologies in the Criminal Procedure Code of the Russian Federation.

Keywords: electronic evidence, cybercrime, criminal procedure, legal assistance in criminal cases.

УДК 343

Иванов Эдуард Александрович

Преподаватель кафедры криминалистики,
Уральский государственный юридический университет
(г. Екатеринбург, Российская Федерация)
edlex@mail.ru

О ТЕНДЕНЦИЯХ К ВЫСТРАИВАНИЮ СИСТЕМЫ ТЕХНОЛОГИЧЕСКОГО ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ЭКСТРЕМИЗМА

Аннотация: Продолжают набирать актуальность вопросы целесообразности внедрения в практику машинного интеллекта, необходимости развития у субъектов правоохранительной деятельности мыслительно-познавательной деятельности в параллели с использованием виртуальных ассистентов. В данной статье рассмотрена уязвимость общества в сетевом пространстве перед проявлением экстремизма. Приведены примеры некоторых зеркальных сдерживающих мер на государственном уровне, свидетельствующих о востребованности межведомственной информационной архитектуры, способной технологически противодействовать возрастающим угрозам.

Ключевые слова: экстремизм, технологии, интернет, инцидент, искусственный интеллект, электронный носитель информации, мобильные устройства и облачные сервера.

Для цитирования:

Иванов Э. А. О тенденциях к выстраиванию системы технологического противодействия угрозам экстремизма // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 401–405.

Последние события, связанные с применением огнестрельного оружия и самодельных взрывных устройств в отношении учащихся образовательных учреждений (организаций), продолжают держать общество в тревоге.

В документах стратегического планирования Российской Федерации¹ отмечается, что несмотря на то, что

количество преступлений экстремисткой направленности достаточно мало по сравнению с общим количеством иных совершаемых на территории Российской Федерации преступлений, однако каждое такое преступление способно вызвать повышенный общественный резонанс и дестабилизировать

¹ Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года: указ Президента Российской Федерации от 29.05.2020 № 344

// СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_353838/ (дата обращения: 20.05.2021).

внутриполитическую обстановку как в отдельном регионе, так и в стране в целом.

Результаты исследований экстремизма, как системы взглядов отдельной группы общества, и терроризма как инструмента устрашения населения, сводятся к тому, что данная категория не склонна к компромиссу, ситуации и социальные явления рассматриваются этими лицами с позиции созданного воображения. Для привлечения в свои ряды новых членов, организации совершения преступлений и распространения экстремисткой идеологии, экстремисты с присущей изощренностью используют уже привычные обществу продукты технологического развития.

Самым распространенным средством связи экстремистских организаций и членов этих организаций стали информационно-телекоммуникационные сети, включая сеть Интернет. До известной степени можно утверждать о том, что угроза терроризма будет сохраняться до тех пор, пока существуют неограниченные возможности доступа к источникам и каналам распространения экстремисткой идеологии.

В конце прошлого столетия компьютеры стали атрибутом быта, ЭВМ интенсивно внедрялись в жизнь практически каждой семьи. Незначительные временные затраты на освоение программных продуктов и их очевидное превосходство перед другими средствами обработки информации привели к интересу «массового» потребителя, что также

обусловило стремительное развитие «софта».

Апогеем развития современной компьютерной техники стали связанные между собой информационными сетями малогабаритные носимые устройства, содержащие в себе не только функции хранения информации и связи, но и фиксирующие множество различной информации, такой как фото- и видеоизображения со встроенной камеры, информация о географическом положении (с помощью встроенных датчиков спутникового позиционирования), данные о скорости движения и др., получаемые с помощью специальных датчиков. Огромные потоки информации ежесекундно формируются, передаются и сохраняются в мобильных устройствах и облачных серверах.

На фоне технологического прорыва субъекты правоохранительной деятельности все чаще стали выявлять новые средства хищения и изменения информации, такое направление в дальнейшем получило характерное название – киберпреступность.

Не остались в стороне и идеологи насилия. Об этом довольно ёмко высказался Председатель Следственного комитета Российской Федерации А. И. Бастрыкин: «Чувствительной темой, вызывающей большую обеспокоенность общества и требующей адекватных мер реагирования со стороны правоохранительных органов, является сращивание террористических и криминальных группировок, расширяющее

логистическое, материальные и технологические возможности экстремистов и террористов»².

Обращают на себя внимание ворвавшиеся в нашу жизнь анонимные транзакции. Набольшее распространение приобрели так называемые криптовалюты³, в частности биткоины⁴. Несмотря на запрет выпуска денежных суррогатов на территории Российской Федерации⁵, ряд факторов, таких как отсутствие: ответственности, валютного контроля и применения законодательства Российской Федерации при трансграничных переводах криптовалюты, способствовал использованию злоумышленниками криптовалюты в целях экстремисткой деятельности, в том числе финансированию терроризма.

² Бастрыкин А. И. О средствах обеспечения безопасности и противодействия экстремизму и терроризму // Вестник Московской академии Следственного комитета Российской Федерации. 2020. № 3. С. 15.

³ Основаны на технологии блокчейн (англ. *blockchain* или *block chain*) – выстроенной по определённым правилам непрерывной последовательной цепочке связанного списка (блоков), содержащих информацию. Копии цепочек хранятся и обрабатываются на множестве разных компьютеров независимо друг от друга. Целостность и хронологический порядок цепочки блоков основаны на криптографии. Наиболее известными разновидностями криптовалюты являются: Bitcoin (Биткоин), Litecoin (Лайткоин) и Ripple (Риппл).

⁴ Биткоин (англ. *Bitcoin*, от *bit* – «бит» и *coin* – «монета») – пиринговая платежная система, использующая одновременно единицу для учета и одноименный протокол передачи данных. Для обеспечения функционирования и защиты используются

В свою очередь, законодатель оперативно рассмотрел вопрос о создании практики внесудебного порядка включения информации в федеральный список экстремистских материалов, а также блокировки доменных имён сайтов, которые пропагандируют насилие⁶.

Однако очевидно, что развитие технологий стремительно опережает своё правовое регулирование.

Технологии анализа данных, оценки и прогнозирования развития ситуаций вносят в нашу жизнь новые свойства машинного обучения – искусственный интеллект. В параллели с научными исследованиями и суждениями об уместности обращения к искусственным нейронным сетям и целесообразности внедрения новых методов (алгоритмов) расследования⁷,

криптографические методы. Биткоины представляют собой расчетные единицы в форме уникальной цепочки цифровых и буквенных знаков, составляющие в совокупности валюту и имеющие ценность только вследствие того, что пользователи готовы платить за них.

⁵ Статья 27 Федерального закона «О Центральном банке Российской Федерации (Банке России)» от 10.07.2002 № 86-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_37570/ (дата обращения: 20.05.2021).

⁶ О противодействии экстремистской деятельности: федеральный закон от 25.07.2002 № 114-ФЗ (изменения в ст. 13 внесены от 08.03.2015 № 23-ФЗ) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_37867/ (дата обращения: 20.05.2021).

⁷ Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2. С. 43–49; Бахтеев Д. В. Предпосылки

значение искусственного интеллекта всерьёз восприняли на государственном уровне⁸. К тому же, 2021 год объявлен Годом науки и технологий⁹. Правительство Российской Федерации последовательно внедряет в собственную структуру современные информационные и аналитические системы управления инцидентами¹⁰. В свою очередь правоохранительные органы и региональные власти принимают меры к созданию самостоятельных информационных центров.

Вместе с тем, опыт расследования данной категории дел, свидетельствует о необходимости пересмотра процессуального порядка получения информации с электронных носителей, в том числе связанных с облачными серверами (хранилищами). Так, следствие

встречается с ситуацией, когда значимая информация удаляется или искажается дистанционно. Несмотря на солидный арсенал технико-криминалистических средств извлечения и анализа цифровых данных, существующее жесткое правовое регулирование на фоне неоднозначного толкования в надзорных и судебных органах, зачастую сводит получение требуемых сведений к области компьютерно-технической экспертизы, что негативно сказывается на сроках расследования и профилактике экстремизма.

Учитывая свойства сетевого пространства и уровень проявления экстремизма, для упреждения этих угроз видится необходимость в продолжении построения межведомственной системы технологического противодействия.

становления и этапы развития технологии искусственного интеллекта // Исторические исследования. 2019. № 8. С. 89–98; Использование методов искусственного интеллекта в изучении личности серийных убийц / Л. Н. Ясницкий, С. В. Ваулева, Д. Н. Сафонова, Ф. М. Черепанов // Криминалистический журнал Байкальского государственного университета экономики и права. 2015. Т. 9, № 3. С. 423–430; Себякин А. Г. Искусственный интеллект к криминалистике: система поддержки принятия решений // Электронный научный журнал Байкальского государственного университета. 2019. Т. 10, № 4. С. 21.

⁸ В. В. Путин в режиме видеоконференции принял участие в основной дискуссии конференции по искусственному интеллекту Artificial Intelligence Journey (AI Journey 2020) на тему «Искусственный интеллект – главная технология XXI века» // Официальный сайт Президента РФ. URL: <http://www.kremlin.ru/events/president/news/64545> (дата обращения: 20.05.2021).

⁹ О проведении в Российской Федерации Года науки и технологий: указ Президента Российской Федерации от 25.12.2020 № 812 // СПС «Гарант». URL: <https://base.garant.ru/400126172/> (дата обращения: 20.05.2021).

¹⁰ О Координационном центре Правительства Российской Федерации: постановление Правительства Российской Федерации от 12.02.2021 № 171 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_377625/92d969e26a4326c5d02fa79b8f9cf4994ee5633b/ (дата обращения: 20.05.2021).

Список литературы

1. Бастрыкин А. И. О средствах обеспечения безопасности и противодействия экстремизму и терроризму // Вестник Московской академии Следственного комитета Российской Федерации. 2020. № 3. С. 11–16.
2. Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2. С. 43–49.
3. Бахтеев Д. В. Предпосылки становления и этапы развития технологии искусственного интеллекта // Исторические исследования. 2019. № 8. С. 89–98.
4. Использование методов искусственного интеллекта в изучении личности серийных убийц / Л. Н. Ясницкий, С. В. Ваулева, Д. Н. Сафонова, Ф. М. Черепанов // Криминалистический журнал Байкальского государственного университета экономики и права. 2015. Т. 9, № 3. С. 423–430.
5. Себякин А. Г. Искусственный интеллект к криминалистике: система поддержки принятия решений // Электронный научный журнал Байкальского государственного университета. 2019. Т. 10, № 4. С. 21.

Eduard A. Ivanov

Lecturer of the Department of Criminalistics,
Ural State Law University
(Yekaterinburg, Russian Federation)
edlex@mail.ru

Abstract: The issues of expediency of introducing machine intelligence into practice, the need to develop mental and cognitive activity in parallel with the use of virtual assistants in law enforcement entities continue to gain relevance. This article examines the vulnerability of society in the network space to the manifestation of extremism. Examples of some mirror deterrent measures at the state level are given, indicating the demand for an interdepartmental information architecture that can technologically counteract increasing threats.

Keywords: extremism, technology, Internet, incident, artificial intelligence, electronic media, mobile devices and cloud servers.

Медведев Виталий Александрович
 Преподаватель кафедры социально-экономических
 и гуманитарных дисциплин,
 Ленинградский областной филиал
 Санкт-Петербургского университета МВД России
 (Ленинградская область, г. Мурино, Российская Федерация)
 smit-vint@yandex.ru

ПРИНЦИП РАБОТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ВЫЯВЛЕНИЯ НАРУШЕНИЙ ПРАВИЛ ДОРОЖНОГО ДВИЖЕНИЯ

Аннотация: В данной статье рассматриваются причины увеличения правонарушений в области дорожного движения, а также методы выявления сотрудниками органов внутренних дел водителей, скрывающихся от оплаты штрафов за нарушение правил дорожного движения или передвигающихся на автомобилях с иностранными регистрационными знаками в нарушение законодательства Российской Федерации.

Ключевые слова: комплексы автоматического контроля, фото- и видеофиксация, нарушение правил дорожного движения, инспектор дорожно-патрульной службы, профилактика и предупреждение правонарушений.

Для цитирования:

Медведев В. А. Принцип работы информационных систем для выявления нарушений правил дорожного движения // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 406–409.

Увеличение камер автоматической фото- и видеофиксации нарушений правил дорожного движения, а также сокращение сотрудников дорожно-патрульной службы приводит к тому, что превышение разрешенного скоростного режима ведет лишь к наложению штрафа. Тем более, что штраф накладывается не на водителя транспортного средства, а на собственника автомобиля. Если рассматривать нарушение скоростного режима на 60–80 км/ч или нарушение более чем на 80 км/ч, то за такие нарушения полагается лишение

водительского удостоверения сроком от четырех до шести месяцев. Однако, если дорожная камера фиксирует, что водитель движется с нарушением скоростного режима на 60–80 км/ч, и этот факт фиксируется исключительно автоматически, то владельцу данного транспортного средства придет штраф на 2,5 тыс. рублей. Хотя ч. 4 ст. 12.9 КоАП предполагает возможность лишения нарушителя водительского удостоверения на срок от четырех до шести месяцев. Если скорость превышена более чем на 80 км/ч, то нарушителя ждет штраф в 5 тыс. рублей при фиксации нарушения

автоматической камерой, а при задержании инспектором ДПС – лишение водительского удостоверения на полгода. За повторное подобное нарушение водителей лишают водительского удостоверения сроком на один год, но в случае автоматической фиксации, все ограничится штрафом в 5 тыс. рублей.

Применить такую меру как лишение права управления транспортным средством можно только, если нарушителя лично задержит инспектор ДПС. Только в таком случае ответственность гарантированно понесет сам нарушитель, а не владелец автомобиля, который мог отдать машину кому-то во временное пользование. Для этого в мегаполисах с развитой инфраструктурой камер автоматической фото- и видеофиксации нарушений правил ПДД каждый год используют систему «Пит-Стоп».

Схема с участием полицейских позволяет наказывать водителей более строго, в отличие от ситуаций, когда нарушения фиксируют исключительно в автоматическом режиме. Такая система нацелена исключительно на фиксацию грубых нарушений, главным образом – превышение скорости на 60-80 км/ч и более.

Принцип работы такой схемы прост. Инспекторы ДПС получают на руки ноутбуки с установленным программным обеспечением «Пит-Стоп». С его помощью полицейские подключаются к одной или сразу нескольким дорожным камерам неподалеку. Как только камеры

зафиксируют грубое нарушение, сотруднику ДПС поступит сигнал. На монитор компьютера можно будет вывести фотографию автомобиля-нарушителя и государственного регистрационного знака, информацию о скорости его движения. Самое главное, что система определяет расчетное время, когда автомобиль будет следовать мимо инспектора ДПС. Обычно при работе с комплексом «Пит-Стоп» инспекторы ДПС занимают позицию в прямой зоне видимости камеры – примерно в 500–700 метрах. Это расстояние как раз позволяет оперативно подготовиться после получения оповещения и выловить машину из потока. При использовании данной системы сотрудники ДПС задерживают водителей за превышение скорости на 60–80 км/ч или более 80 км/ч, а также за повторное превышение свыше 80 км/ч. Соответственно, каждого из задержанных лишают водительского удостоверения.

Также систему «Пит-Стоп» можно использовать в комплексе с системой автоматической фиксации передвижения транспортных средств. Такие системы имеют широкое распространение в мегаполисах. Зачастую грубые нарушения скоростного режима также приходится на большие города нашей страны, такие как Москва и Санкт-Петербург. Благодаря работе в комплексе двух систем можно не только выявлять грубые нарушения скоростного режима в реальном времени, но и выявлять конкретных злостных нарушителей на автомобильных дорогах.

При использовании системы автоматической фиксации передвижения транспортных средств можно выявить маршруты передвижения злостных нарушителей, которые уходят от лишения водительского удостоверения, а ограничиваются только уплатой штрафа. Существует целая база таких нарушителей.

Не стоит забывать о нарушениях правил дорожного движения, совершаемых на автомобилях с иностранными регистрационными номерами. Раньше среди водителей считалось, что на таких автомобилях нарушение ПДД остается безнаказанным по причине отсутствия регистрации таких транспортных средств на территории России.

Однако, в настоящее время, все чаще и чаще на дорогах мегаполисов сотрудники ГИБДД устраивают рейды именно на остановку таких автомобилей. Соответственно, сотрудники ДПС, имея данные по таким нарушителям и используя две системы в комплексе, смогут выявлять таких нарушителей на дорогах и привлекать к административной ответственности, в том числе с возможностью лишения водительских удостоверений. Водитель после остановки сотрудниками ГИБДД получает постановления об административном наказании за несоблюдение ПДД, а транспортное средство отправляется на штраф стоянку, пока собственник автомобиля не оплатит все штрафы.

Список литературы

1. Повышение эффективности и контроля за выполнением водителями правил дорожного движения / О. М. Астафьева, О. С. Гасилова, О. Ю. Грехов, Б. А. Сидоров // Современные проблемы науки и образования. 2015. № 1-1.
2. Головки В. В. Обеспечение безопасности дорожного движения в государственной системе профилактики правонарушений / В. В. Головки, О. И. Бекетов, В. И. Майоров // Наука и практика. 2016. № 3 (68). С. 33–39.
3. Майоров В. И. Правовые проблемы применения специальных технических средств автоматической фотовидеофиксации нарушений правил дорожного движения / В. И. Майоров, А. Д. Дымберов, П. В. Молчанов // Юридическая наука и правоохранительная практика. 2016. № 3 (37). С. 69–77.

Vitaly A. Medvedev

Lecturer of the Department of Socio-economic and Humanitarian Disciplines,
Leningrad Regional branch
St. Petersburg University of the Ministry of Internal Affairs of Russia
(Leningrad region, Murino, Russian Federation)
smit-vint@yandex.ru

**THE PRINCIPLE OF FUNCTIONING OF INFORMATION SYSTEMS FOR
DETECTING VIOLATIONS OF TRAFFIC RULES**

Abstract: This article discusses the reasons for the increase in traffic offenses, as well as methods for identifying drivers who are hiding from paying fines for violating traffic rules or driving cars with foreign registration plates in violation of the legislation of the Russian Federation.

Keywords: automatic control systems, photo and video recording, violation of traffic rules, inspector of the road patrol service, prevention and prevention of offenses.

Очеретько Елена Александровна

Кандидат юридических наук, доцент кафедры гражданского и
предпринимательского права,
Елецкий государственный университет им. И. А. Бунина
(г. Елец, Российская Федерация)
Lena.ocheretko@yandex.ru

Попова Анна Алексеевна

Студент,
Елецкий государственный университет им. И. А. Бунина
(г. Елец, Российская Федерация)
nura.d2015@yandex.ru

**РОЛЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАССЛЕДОВАНИИ
НЕРАСКРЫТЫХ ПРЕСТУПЛЕНИЙ ПРОШЛЫХ ЛЕТ**

Аннотация: Нераскрытые преступления прошлых лет – одна из актуальных проблем на сегодняшний день для всей правоохранительной системы. Она требует особого внимания и разрешения. В связи с этим активно проводятся различные криминалистические исследования, разработки в области судебной медицины, внедряются новейшие технологии и технические установки в этой сфере. В данной статье рассмотрены современные методы и средства, применяемые правоохранительными органами для раскрытия преступлений, а также даётся оценка перспективы их развития на ближайшие годы.

Ключевые слова: преступления прошлых лет, современные технологии, технические средства, криминалистика, исследования, компьютерные системы.

Для цитирования:

Очеретько Е. А. Роль информационных технологий в расследовании нераскрытых преступлений прошлых лет / Е. А. Очеретько, А. А. Попова // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 410–415.

Ежедневно в России совершаются тысячи различных преступлений, каждое из которых требует немедленного рассмотрения, а впоследствии и разрешения. Но, как показывает статистика, лишь половина регистрируемых из них раскрывается, что ведёт к неумолимому росту преступлений

прошлых лет. Тем не менее, работа с данной категорией преступлений не прекращается. Активно ведётся внедрение компьютерных, судебно-медицинских и иных технологий в данную область деятельности.

На сегодняшний день в регионах России создаются целые подразделения по раскрытию

преступлений прошлых лет. Так, например, такое подразделение в СК по Иркутской области смогло раскрыть преступление 16-летней давности и задержать подозреваемого, обвиняемого в убийстве маленькой девочки. И таких примеров немало. За последние годы наблюдается положительная динамика в раскрытии дел, поднятых из архивов. Большая роль в этом принадлежит современным технологиям, используемым в следственной деятельности.

Изучая методику раскрытия преступлений прошлых лет, необходимо начать с определения этой категории. Традиционно к ним относят:

- преступления, по которым было приостановлено следствие по каким-либо законным основаниям;
- преступления, выявление которых произошло лишь спустя длительное время после их совершения;
- преступления, которые совершались долгое количество времени (серийные преступления).

Иными словами, **преступлениями прошлых лет** следует понимать совершенные и зарегистрированные в установленном порядке в прошлые годы преступления, предварительное следствие по которым приостановлено на основании п. 1 ч. 1 ст. 208 УПК, но не истекли сроки давности привлечения к уголовной ответственности¹.

В своем недавнем выступлении Председатель Следственного комитета РФ А. И. Бастрыкин обозначил, что раскрытие преступлений прошлых лет – один из главных приоритетов деятельности следственных органов. Чем же вызвана актуальность данной проблемы? Прежде всего, это связано с необходимостью обеспечения важного принципа – неотвратимости наказания. Виновный должен быть обязательно наказан. Иначе это может привести к снижению авторитета государственной власти у населения и возникновению чувства вседозволенности. К тому же преступник, разгуливающий на свободе, ощущая свою безнаказанность, может продолжить совершать преступные деяния и подавать тем самым пример другим. Все это приводит к возникновению серийного характера преступности и роста числа преступлений в целом.

Тем не менее, за последние годы был раскрыт ряд ранее приостановленных преступлений. В возобновлении и их успешном раскрытии помогли современные технологии, а также сплоченная работа Следственного комитета РФ и МВД РФ. Сегодня проводить расследование помогают новейшие технологии, о существовании которых не могли даже мечтать 20–30 лет назад.

Большим прорывом в данной области стала генотипоскопическая экспертиза². Если ранее работники

¹ Седова Г. И., Степанов В. В. Дознание в правоохранительных органах. Учебное пособие. М.: Юрайт, 2019. С. 130.

² Кирюхин Д. А. Географическое профилирование – помощь в составлении психологического профиля преступника и

следственных органов и органов дознания, обнаружив следы крови на месте преступления, могли лишь сравнить ее с группой крови подозреваемого, то сегодня исследование ДНК позволяет определить не только вид биологических улик (пот, слюна, кровь), но и лицо, которому они принадлежат.

Не каждый знает, что в современных правоохранительных органах существуют целые банки генетических данных. Здесь хранятся образцы ДНК, как подозреваемых, обвиняемых, осужденных, так и просто людей, проходивших свидетелями по какому-либо делу. Количество сохраняемых биоматериалов исчисляется сотнями тысяч. Это объясняется тем, что лишь по одному делу может быть проведено более тысячи всевозможных генетических проб. Получается, что данный метод значительно ускоряет процесс установления личности преступника, так как ни одно преступление не может пройти бесследно – биологические следы остаются всегда.

Говоря о компьютерных технологиях, следует упомянуть о существовании в правоохранительной системе различных автоматизированных банков данных (АБД). Свое развитие получила автоматизированная система Следственного комитета «СТРАС-

СК», а также различные специализированные базы данных ГИЦ МВД³. Подобные системы активно и успешно используются уже несколько лет, позволяя быстро получать доступ к информации о нераскрытых преступлениях, об опасных серийных преступниках, рецидивистах, похищенных предметах и др. Данные, содержащиеся в них, непосредственно помогают при расследовании преступлений.

Отдельное внимание стоит уделить гипнорепродукторам. Это специалисты, которые с помощью применения психотехник (гипноза) восстанавливают у человека воспоминания, очищают их от надуманного, воспроизводят в памяти какие-либо детали или моменты. Такая методика очень важна для расследования преступлений прошлых лет. Следовательно, возобновляя старое дело, обязан вновь опрашивать свидетелей, заново восстанавливать картину произошедшего. Но зачастую человек попросту забывает какие-то детали, либо придумывает⁴.

Ещё одной проблемой является нежелание лиц, участвующих в деле, сотрудничать со следствием. Вызвано это тем, что люди перестают верить в возможность спустя время найти какие-то новые доказательства, которые бы помогли успешному разрешению дела. Что касается

поиска мест сокрытия трупов // Эксперт-криминалист. 2018. № 4. С. 6–8.

³ Шарыпова В. А., Темерев Г. В. Роль информационных технологий в профессиональной деятельности юриста // Форум молодых ученых. 2018. № 4 (20). С. 1564–1567.

⁴ Лозовский Д. Н., Ульянова И. Р. Актуальные вопросы расследования нераскрытых преступлений прошлых лет // Общество и право. 2019. № 4 (62). С. 135–137.

родственников потерпевших, то часто им сложно вспоминать произошедшее, поэтому они предпочитают смириться с фактом безнаказанности преступника, чем заново переживать ту моральную боль.

Тем не менее, метод гипнорепродукции широко применяется, причем весьма успешно. Так, гипнорепродуктор из центрального аппарата СК РФ поспособствовал раскрытию убийства 6-летней девочки в городе Зима Иркутской области. Специалист помог свидетелю восстановить в памяти все детали произошедшего и даже составить фоторобот преступника.

Далеко вперед продвинулись и технологии в криминалистике. Широко применяемые в качестве основных доказательств отпечатки пальцев удастся найти на таких поверхностях, которые не представлялось даже возможным ранее исследовать. Это происходит с использованием специальных камер (цианоакрилатные и нингидрированные). Также появились такие специальные криминалистические устройства, как детекторы взрывчатых веществ, магнитометры, металлодетекторы. С их помощью удастся обнаруживать огнестрельное оружие, частицы взрывчатых веществ. Все вышеперечисленные технологии в совокупности позволяют значительно повысить эффективность расследования преступлений⁵.

Анализируя вышеизложенное, можно сделать вывод, что технологии, применяемые сегодня правоохранительными органами при расследовании преступлений, за последние годы были высоко усовершенствованы, что позволяет поднимать из архивов преступления прошлых лет и проводить их расследование на новом уровне. Этот фактор позволяет повысить положительную статистику раскрытия данной категории преступлений в разы. Но тут же возникает вопрос: каковы перспективы расследования старых преступлений на ближайшие годы?

Изучив статистику минувшего года, мы видим, что за 2020 год было раскрыто 3,6 преступлений прошлых лет, а это на 6 % больше, чем в 2019 году. Если рассматривать данные за 2006 год, то следует отметить, что количество нераскрытых преступлений уменьшилось в 4 раза. Глава СК РФ А. И. Бастрыкин в своем выступлении отметил, что необходимо продолжать улучшать статистику, постепенно разрабатывать и внедрять новое оборудование, технические средства и др., т. к. такая положительная динамика – это заслуга органов дознания и новых экспертных технологий.

Уже сегодня ведется разработка новых и совершенствование существующих экспертных методик, чем занимается Научно-исследовательское управление (НИИ криминалистики) и Управление организации экспертной деятельности

⁵ Лозовский Д. Н., Ульянова И. Р. Актуальные вопросы расследования нераскрытых преступлений прошлых лет //

Общество и право. 2019. № 4 (62). С. 135–137.

совместно с другими подразделениями полиции и Следственного комитета РФ⁶. Например, активно исследуются новые объекты и методы проведения почерковедческих экспертиз, подготовлены методические рекомендации по особенностям назначения судебно-экологических, а также оценочных (стоимостных) экспертиз и исследований. Немалый интерес представляют технические возможности систем лазерного 3D-сканирования места происшествия, которые позволяют с высочайшей точностью получать информацию с места происшествия в виде трехмерной модели.

Таким образом, расследование преступлений прошлых лет – это

долгий и сложный процесс, требующий высокой концентрации всех возможных сил, начиная от человеческого фактора и заканчивая новейшими технологиями. Только такая сосредоточенная работа может привести к успешному завершению дела. Следователям, расследующим уголовные дела по преступлениям прошлых лет, особенно необходимо использовать в своей деятельности все существующие технологии, ведь это кардинально влияет на результат расследования. Только ломая традиционные представления о путях достижения цели расследования, можно добиться высоких результатов в расследовании преступлений.

Список литературы

1. Головка Л. В. Судоустройство и правоохранительные органы. Краткий курс. Учебное пособие / Л. В. Головка, Л. В. Брусницын, Г. Н. Ветрова. М.: Городец, 2020.
2. Кирюхин Д. А. Географическое профилирование – помощь в составлении психологического профиля преступника и поиска мест сокрытия трупов // Эксперт-криминалист. 2018. № 4. С. 6–8.
3. Лозовский Д. Н. Актуальные вопросы расследования нераскрытых преступлений прошлых лет / Д. Н. Лозовский, И. Р. Ульянова // Общество и право. 2019. № 4 (62). С. 135–137.
4. Правоохранительные органы России. Учебник для вузов. М: Юрайт, 2019.
5. Седова Г. И. Дознание в правоохранительных органах. Учебное пособие / Г. И. Седова, В. В. Степанов. М.: Юрайт, 2019.
6. Шарыпова В. А. Роль информационных технологий в профессиональной деятельности юриста / В. А. Шарыпова, Г. В. Темерев // Форум молодых ученых. 2018. № 4 (20). С. 1564–1567.

⁶ Правоохранительные органы России. Учебник для вузов. М: Юрайт, 2019. С. 296.

Elena A. Ocheretko

PhD (Law), Associate Professor of the Department of Civil and Business Law,
Yelets State University named after I. A. Bunin
(Yelets, Russian Federation)
Lena.ocheretko@yandex.ru

Anna A. Popova

Student,
Yelets State University named after I. A. Bunin
(Yelets, Russian Federation)
nura.d2015@yandex.ru

THE ROLE OF INFORMATION TECHNOLOGY IN THE INVESTIGATION OF UNSOLVED CRIMES OF THE PAST

Abstract: Unsolved crimes of the past years are one of the most pressing problems for the entire law enforcement system today. It requires special attention and permission. In this regard, various forensic studies and developments in the field of forensic medicine are being actively carried out, and the latest technologies and technical installations in this area are being introduced. This article examines modern methods and tools used by law enforcement bodies to disclose crimes, and also assesses the prospects for their development in the coming years.

Keywords: crimes of the past, modern technologies, technical means, criminalistics, research, computer systems.

Иванов Владислав Юрьевич

Преподаватель кафедры криминалистики,
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
blad02051995@mail.ru

Соколова Алёна Станиславовна

Курсант,
Уральский юридический институт МВД России
(г. Екатеринбург, Российская Федерация)
alyona.sokolova.2018@mail.ru

ОСОБЕННОСТИ ДОПРОСА ЛИЦ, НАХОДЯЩИХСЯ НА САМОИЗОЛЯЦИИ В УСЛОВИЯХ ПАНДЕМИИ COVID-19

Аннотация: В статье произведён анализ законопроекта, предусматривающий введение статьи 189.1 «Особенности допроса свидетеля посредством видео-конференц-связи» в действующий УПК РФ. Рассмотрена целесообразность данных поправок в условиях пандемии коронавирусной инфекции. Произведен анализ положений текста данного законопроекта и позиции законодателя. Высказано аргументированное мнение авторов статьи относительно необходимости скорейшего введения данной нормы в условиях пандемии COVID-19 вызванной коронавирусом SARS-CoV-2.

Ключевые слова: видео-конференц-связь, дистанционный допрос, коронавирус, пандемия, COVID-19, самоизоляция.

Для цитирования:

Иванов В. Ю. Особенности допроса лиц, находящихся на самоизоляции в условиях пандемии COVID-19 / В. Ю. Иванов, А. С. Соколова // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 416–422.

Современное общество развивается быстрыми темпами в сторону по цифровизации большинства сфер жизнедеятельности человека. Новые технологии, так или иначе, проникают в различные практические сферы, в том числе и в

деятельность по расследованию уголовных дел. Так, ещё в 2011 году были внесены изменения в ст. 240 Уголовно-процессуального кодекса Российской Федерации¹, а также была введена статья 278.1 УПК РФ². Данные нормы позволили суду

¹ Далее – УПК РФ.

² О внесении изменений в Уголовно-процессуальный кодекс Российской

производить допрос свидетелей и потерпевших посредством использования системы видео-конференц-связи.

Судебная практика свидетельствует, что данная норма активно применяется в практической деятельности и способствует реализации таких процессуальных принципов, как рассмотрение дела в разумный срок, полное и всестороннее исследование всех обстоятельств уголовного дела и минимизирует время следователя (дознателя).

Анализ становления правовых основ использования видео-конференц-связи в сфере уголовного судопроизводства показывает, что эта современная и эффективная технология в Российской Федерации применяется повсеместно, и ее преимущества зримо отражаются в статистических показателях о деятельности судов общей юрисдикции. По официальным данным, в судах общей юрисдикции ежегодно проводится более 800 сеансов связи более чем в 160 000 судебных процессах в год. В течение 13 лет произведено более 650 000 видеоконференций³.

Современное общество в 21-м веке во всём мире столкнулось со значительной проблемой, поработившей практически весь мир. Пандемия COVID-19, вызванная коронавирусом SARS-CoV-2, во многом вызвала сбой в привычном

образе жизни граждан практически всех стран, затронув все сферы жизнедеятельности. Безусловно, данная проблема затронула и органы государственной власти. Правоохранительным органам стало сложнее и опаснее работать в новых реалиях, так как данная инфекция нового типа смогла подтолкнуть криминальный мир к увеличению преступности в информационно-телекоммуникационной сфере. В настоящее время преступления в сфере IT-технологий стали привычным явлением, поскольку определенная часть людей перешла на удалённую работу и свою профессиональную деятельность осуществляют дистанционно.

Некоторая часть людей находится на самоизоляции в связи с подтвержденным диагнозом коронавирусной инфекции, а также пребывают по месту жительства по случаю контактирования с такими людьми. Данные лица могут находиться в каком-либо процессуальном статусе при осуществлении расследования по уголовному делу, что соответственно затрудняет производство следственных действий с их участием.

В настоящее время уголовно-процессуальное законодательство нуждается в изменениях по предоставлению возможности следователю (дознателю)

Федерации: федеральный закон от 20 марта 2011 г. № 39-ФЗ // Собр. законодательства Рос. Федерации. 28.03.2011. № 13. Ст. 1686.

³ Поддубняк А. А. Допрос свидетеля посредством видео-конференц-связи на стадии предварительного расследования как

новелла Российского законодательства / А. А. Поддубняк, И. С. Евдокимова // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2018. Т. 4 (70), № 3. С. 160.

производить следственные действия в режиме видео-конференц-связи.

Действительно, данный положительный опыт использования видео-конференц-связи в суде целесообразно перенять и на досудебную стадию уголовного судопроизводства.

Разработка данной нормы в законодательных органах ведётся относительно давно, но в настоящее время, поправки не вступили в силу. Предложенные изменения значительно облегчат работу следователям, будут способствовать более качественному и эффективному расследованию преступлений и сократят срок производства по уголовному делу.

Нельзя не согласиться с мнением председателя Комитета Совета Федерации по экономической политике А. В. Кутеповым, который подготовил данный проект поправок в УПК РФ, по его мнению: «такой шаг избавит правоохранительную систему от лишних материальных и временных затрат, так как неявка свидетелей или потерпевших, проживающих в другом городе или регионе, становится весомым основанием для бесконечных продлений сроков следствия»⁴.

Положительно поправки отметил и статс-секретарь Федеральной палаты адвокатов К. Э. Добрынин, пояснив, что «введение дистанционной формы допроса также позволит обезопасить свидетелей в том числе от внепроцессуального давления»⁵.

Предполагается, что изменения в уголовно-процессуальном законе коснутся ст. 5 УПК РФ, которая дополнится п. 8.1 следующего содержания «допрос посредством видео-конференц-связи – это допрос, который проводится с использованием технических средств и программного обеспечения для персонального компьютера, мобильных устройств и браузера, обеспечивающих передачу звука и изображения в реальном времени»⁶.

По нашему мнению, данные поправки являются как никогда актуальными в период пандемии COVID-19. В рассматриваемом случае дополнения нового положения в УПК РФ значительно помогло бы в работе следователю (дознавателю). Производство следственного действия как допрос с человеком, находящимся на самоизоляции, было бы крайне сложным без видео-конференц-связи. Также допрос лица дистанционным

⁴ Проект поправок в УПК, предусматривающих онлайн-допросы свидетелей и потерпевших, доработан // Адвокатская газета. 2020. 6 ноя. URL: <https://www.advgazeta.ru/novosti/proekt-popravok-v-upk-predusmatrivayushchikh-onlayn-doprosy-svidetelej-i-poterpevshikh-dorabotan/> (дата обращения: 14.05.2021).

⁵ Проект поправок в УПК, предусматривающих онлайн-допросы свидетелей и потерпевших, доработан // Коллегия адвокатов «Таможенный адвокат».

Дата обновления: 06.11.2020. URL: <http://www.customs-advocate.ru/ru/news/sendvalues/more/2582/> (дата обращения: 14.05.2021).

⁶ Предлагается разрешить следствию проводить допросы свидетелей по видео // Российская газета. URL: <https://rg.ru/2020/10/29/sledstviu-mogut-razreshit-provodit-doprosy-svidetelej-po-videosviasi.html> (дата обращения: 14.05.2021).

образом посредством современных технологий имеет существенные плюсы и преимущества. Использование систем видео-конференц-связи не только в суде, но и на стадии предварительного расследования:

- будет способствовать осуществлению уголовного судопроизводства в разумный срок;
- производство допроса при помощи систем видео-конференц-связи помогло бы допрашиваемым лицам находиться в комфортной для них обстановке для дачи показаний;
- использование данных систем видео-конференц-связи способствовало бы получению наиболее полных, достоверных, информативных показаний со стороны допрашиваемого лица;
- полученные с помощью системы видео-конференц-связи показания, помогут следователю в составлении не только процессуальных документов (протокол допроса), но и также будут фиксироваться посредством записи произведенного допроса. В свою очередь запись отражала бы все действия со стороны следователя и допрашиваемого лица. Также данная запись исключала бы возможность подачи жалобы на неправомерные действия следователя при производстве следственного действия. Ведь на записи отражались бы все этапы производимого следственного действия (допроса лица).

Не следует забывать, что в данном случае также видео-конференц-связь имеет место быть при допросе лица, который болеет коронавирусной инфекцией. Участие

в допросе в период пандемии может быть сопряжено с угрозой заражения COVID-19 других участников уголовного судопроизводства, поскольку допрашиваемому потребуется нарушить режим самоизоляции, добраться до следственного отдела, длительное время присутствовать на допросе в замкнутом пространстве, а затем возвращаться домой. Проблема становится еще более актуальной, когда допрашиваемое лицо относится к группе риска по коронавирусной инфекции (возраст старше 65 лет, наличие ряда хронических заболеваний). В данной ситуации представляется разумным заявить ходатайство об отложении допроса до окончания действия ограничительных мер по распространению коронавирусной инфекции, либо проводить допрос посредством видео-конференц-связи, если самочувствие допрашиваемого лица позволит провести данное следственное действие.

На основании всего вышесказанного следует учесть, что со временем мир прогрессирует и растет в сфере компьютерных технологий, правда, касается этот прогресс не все стороны жизни человечества. Настоящее законодательство бы сильно пострадало от внесения постоянных новшеств в законодательство на фоне прогрессирования общества и мира в целом. Уголовно-процессуальное законодательство также меняется на фоне развития общества, но следует сказать, что пробелы в нормах остаются и по сей день, также возможны противоречия в нормах.

Одним из противоречий как раз и выступает видео-конференц-связь, так как данное понятие введено в УПК РФ, правда используется не в отношении всех участников уголовного судопроизводства и не на всех стадиях. Например, видео-конференц-связь чаще всего применяют на станциях апелляционного производства и в нормах УПК РФ об этом сказано. Почему же нельзя вести данный процесс в настоящее время на все стадии уголовного судопроизводства? Во время пандемии коронавирусной инфекции? Ответ на данный вопрос пока невозможно дать в связи с малым процентным соотношением таких ситуаций с лицами, участвующими в уголовном судопроизводстве с диагнозом коронавирусной инфекции.

Следует отметить, законопроект о возможности производства допроса по видео-конференц-связи несет в себе действительно позитивный мотив, данное новшество помогло бы следователям (дознателям) в производстве следственного действия. Следует сказать, что видеосвязь существовала и раньше, например, иной раз она помогала в построении диалога с лицом, находящимся в местах лишения свободы, который не имеет возможности присутствовать в зале суда. Данное новшество позволит допрашивать свидетелей посредством видео-конференц-связи на стадии предварительного следствия с соблюдением основных правил и требований производства расследования по уголовному делу и с учетом особенностей допроса несовершеннолетних лиц.

Видео допрос свидетеля сократил бы срок предварительного расследования, так как существуют ситуации, когда свидетель может находиться на большом удалении от органа предварительного следствия, а это, в свою очередь, может служить поводом для продления разумного срока. Став очевидцем преступления в одном регионе Российской Федерации, лицо по личным обстоятельствам может его покинуть (возвращение в место постоянного проживания, переезд на постоянное место жительства, командировка, отбывание наказания и др.), что делает достаточно затруднительным обеспечение явки свидетеля к следователю для допроса. Выезд следователя в местонахождение свидетеля требует дополнительных временных и материальных затрат. При этом не стоит забывать, что у следователя в производстве находится не одно уголовное дело и выезд следователя для допроса одного свидетеля будет также затягивать сроки расследования по другим уголовным делам.

Несомненно, следует указать о полезности использования видео-конференц-связи при заболевании коронавирусной инфекцией, так как данная пандемия поработила большую часть населения и поставила некоторые сферы деятельности в состояние регресса. В данном случае видео-конференц-связь помогла бы помочь следователю взаимодействовать со всеми участниками уголовного судопроизводства, которые находятся на самоизоляции с диагнозом коронавирусной инфекции.

Подводя итог вышесказанному, следует отметить, что данная норма была бы отличным помощником в уголовном судопроизводстве, тем более в настоящее время, а именно в период пандемии, посредством которой весь мир работает

посредством технических средств. Следственное действие как допрос стал бы проводиться намного экономичнее как с точки зрения финансовой составляющей, так и времени следователя.

Список литературы

1. Новиков С. А. Допрос с использованием систем видео-конференц-связи: завтрашний день российского предварительного расследования // Российский следователь. 2014. № 1. С. 2–6.

2. Поддубняк А. А. Допрос свидетеля посредством видео-конференц-связи на стадии предварительного расследования как новелла Российского законодательства / А. А. Поддубняк, И. С. Евдокимова // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2018. Т. 4 (70), № 3. С. 159–165.

3. Предлагается разрешить следствию проводить допросы свидетелей по видео // Российская газета. URL: <https://rg.ru/2020/10/29/sledstviu-mogut-razreshit-provodit-doprosy-svidetelej-po-videosviasi.html>.

4. Проект поправок в УПК, предусматривающих онлайн-допросы свидетелей и потерпевших, доработан // Адвокатская газета. 2020. 6 ноя. URL: <https://www.advgazeta.ru/novosti/proekt-popravok-v-upk-predusmatrivayushchikh-onlayn-doprosy-svideteley-i-poterpevshikh-dorabotan/>.

5. Проект поправок в УПК, предусматривающих онлайн-допросы свидетелей и потерпевших, доработан // Коллегия адвокатов «Таможенный адвокат». Дата обновления: 06.11.2020. URL: <http://www.customs-advocate.ru/ru/news/sendvalues/more/2582/>.

Vladislav Yu. Ivanov

Lecturer at the Department of Forensic Science,
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
blad02051995@mail.ru

Alena S. Sokolova

Student,
Ural Law Institute of the Ministry of Internal Affairs of Russia
(Yekaterinburg, Russian Federation)
alyona.sokolova.2018@mail.ru

FEATURES OF INTERROGATION OF PERSONS IN SELF-ISOLATION IN THE CONDITIONS OF THE COVID-19 PANDEMIC

Abstract: The article analyzes the draft law providing for the introduction of Article 189.1 «Peculiarities of interrogating a witness by means of videoconferencing» into the current Criminal Procedure Code of the Russian Federation. The feasibility of these amendments in the context of a coronavirus pandemic was considered. The analysis of the provisions of the text of this draft law and the position of the legislator is made. A reasoned opinion was expressed by the authors of the article regarding the need for the early introduction of this norm in the context of the COVID-19 pandemic caused by the SARS-CoV-2 coronavirus.

Keywords: video conferencing, distance interrogation, coronavirus, pandemic, COVID-19, self-isolation.

УДК 343.9

Каравая Анастасия Владимировна

Ассистент кафедры «Цифровая криминалистика»,
Московский государственный технический университет имени Н. Э. Баумана
(национальный исследовательский университет)
(г. Москва, Российская Федерация)
karlova_av@bmstu.ru

ЦИФРОВИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Аннотация: Статья посвящена некоторым аспектам использования цифровых технологий в деятельности правоохранительных органов. Люди все чаще полагаются на технологии в повседневных потребностях, начиная от коммерции до социального взаимодействия. Для большинства людей технологии являются неотъемлемой частью повседневной жизни. В статье описывается влияние процесса цифровизации на деятельность правоохранительных органов, так как в первую очередь современные технические средства должны быть использованы для расследования, раскрытия и предупреждения преступлений. В статье также рассматриваются аспекты использования электронных доказательств в уголовном процессе Российской Федерации и зарубежных стран. На данный момент компьютеризация и информатизация деятельности правоохранительных органов имеет важное значение. В тоже время цифровые технологии предоставляют широкие возможности в использовании информационных ресурсов. Исходя из этого, основная цель использования информационных технологий и средств компьютерной техники – это повышение эффективности механизмов анализа и скорости обработки информации с целью расследования, раскрытия и предупреждения преступлений.

Ключевые слова: цифровизация, правоохранительные органы, киберпреступность, цифровые технологии, электронные доказательства, электронное средство доказывания.

Для цитирования:

Каравая А. В. Цифровизация деятельности правоохранительных органов // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 423–428.

На современном этапе общественного
развития научно-технический

прогресс оказывает влияние на все
сферы человеческой деятельности¹. А

¹ Карлова А. В. Метод 3D-моделирования в современной судебной экспертизе // MODERN SCIENCE. 2020. №1-3. С. 81.

также и в деятельность правоохранительных органов, куда интегрируются новые достижения развивающихся техники и науки.

В настоящее время значительно растет уровень преступности, а преступники находят все более изощренные способы обмануть законодательство и замаскировать свои преступные действия. В век современных технологий технические средства также активно используются злоумышленниками. Этот рост привел к растущей зависимости от технологий и, в свою очередь, к расширению криминогенных возможностей, известных теперь как «киберпреступность».

Развитие сети Интернет открыло относительно небезопасную среду для криминальной эксплуатации, объединив миллиарды пользователей и сделав их потенциальными целями.

Традиционные подходы к борьбе с преступностью чреваты трудностями во взаимосвязанном мире технологий, в котором мы сейчас живем. Правоохранительные органы, которые имеют основной мандат на борьбу с преступностью и играют важную роль в предупреждении преступности, работают в основном в контексте выявления и задержания преступников. Методы действий киберпреступников часто делают традиционные методы работы полиции неэффективными. Анонимность, которую обеспечивает сеть Интернет правонарушителям, географическая разбросанность правонарушителей и потерпевших, а

также правонарушители, обычно находящиеся за пределами юрисдикции, – все это делает киберпреступность сложной задачей для правоохранительных органов.

Колоссальное развитие информационных технологий приводит к тому, что в своей повседневной жизни человек постоянно использует различные компьютерные устройства. Информационное содержимое, получаемое при исследовании компьютерных устройств, представляет значительный интерес при расследовании уголовных дел.

Особую актуальность имеет применение электронных доказательств в уголовном судопроизводстве России и зарубежных стран.

Использование электронных доказательств в уголовном судопроизводстве становится привычным делом. Одновременно в криминалистике информационные технологии все чаще становятся предметом научных изысканий².

Доказательствами в уголовном деле все чаще становятся электронные записи, сообщения, файлы, находящиеся на электронных носителях. Процессуально значимые объекты появляются не только при совершении киберпреступлений. «Любое из обстоятельств, подлежащих доказыванию, в наше время может быть представлено в цифровой форме». Электронное доказательство на сегодня – это условное обозначение доказательства,

² Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / С. В. Зуев [и др.]; ответственный

редактор С. В. Зуев. Москва: Издательство Юрайт, 2021. С. 7.

содержание которого представлено в электронном виде. Такое положение дел сохраняется из-за отсутствия законодательного закрепления данной категории.

Электронные свидетельства – категория гораздо шире, и может включать в себя записи, хранящиеся, например, сетевыми или интернет-провайдерами. Такие данные могут быть использованы в доказывании при соблюдении ряда условий. Доказательства, кроме того, всегда должны отвечать четким критериям допустимости. Чтобы перевести электронную информацию в электронные доказательства, требуется надлежащее правовое регулирование и конкретные юридические нормы. Это во многом объясняет, почему электронное доказывание сейчас находится на стадии осмысления и теоретического обоснования. Тем не менее юридическая практика развивается и в настоящее время нуждается в рекомендациях, основанных на обобщении положительного опыта работы с электронными средствами доказывания.

Электронные средства доказывания – это любые правовые информационные технологии, закрепленные в уголовно-процессуальном законодательстве, используемые при доказывании по уголовным делам для получения и проверки цифровой информации³.

Интересен также зарубежный опыт применения электронных доказательств в уголовном судопроизводстве.

Например, судебный уголовный процесс США активно применяет новейшие технические разработки, позволяющие трансформировать процесс доказывания по уголовным делам и оптимизировать ряд процессуальных и организационных действий. Применение современных информационных технологий в уголовном процессе предполагает наличие необходимого информационного уровня грамотности его участников: свидетелей, потерпевших, подозреваемых⁴.

В Великобритании активно применяют электронные устройства и технологии при расследовании преступлений, обнаружении преступных следов, производстве следственных действий. Путем применения электронных устройств фиксируются доказательства, которые затем используются стороной обвинения в суде при даче показаний.

В Канаде применяется онлайн регистрация и отслеживание поданных процессуальных документов, а при помощи Веб-интерфейса участники судопроизводства могут детально ознакомиться с материалами уголовного дела.

³ Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / С. В. Зуев [и др.]; ответственный редактор С. В. Зуев. Москва: Издательство Юрайт, 2021. С. 11–12.

⁴ Информационные технологии в уголовном процессе зарубежных стран. Монография /

Коллектив авторов; под ред. С. В. Зуева. М., 2020. 216 с. Режим доступа: Международная ассоциация содействия правосудию. URL: <http://www.iuaj.net/node/2795> (дата обращения 16.05.2021).

В Германии и Австрии используют систему искусственного интеллекта, когда в ходе расследования преступлений применяется автоматизированный розыск по электронным архивам уголовных дел. Данные, содержащиеся в информационной базе о совершении преступления, сравниваются со сведениями из других баз данных с целью установления подозреваемого в конкретном преступлении.

В Швейцарии информационные технологии активно используются на досудебной и судебной стадиях уголовного процесса при производстве следственных действий, например, видеоконференции в ходе проведения допроса, если явка допрашиваемого лица невозможна либо требует больших судебных расходов⁵.

Во Франции развита система акустического и визуального наблюдения, применяемая сотрудниками полиции по решению суда, предполагающая применение аудио- и фото-фиксации в транспортных средствах, жилых помещениях для установления информации, полученной из переговоров подозреваемого с другими лицами.

Интересен передовой опыт Китая по оптимизации уголовного процесса и применении видеозаписи проводимых следственных действий, когда используют специально созданные интернет-платформы и облачные хранилища для обмена процессуальными документами⁶.

Эти передовые информационные технологии, бесспорно, позволят сократить бюрократические процессуальные процедуры и будут способствовать сосредоточению следователей только на расследовании уголовных дел.

В зарубежных странах по-разному решается вопрос с допустимости электронных доказательств. Например, в Японии электронные документы, признаются подлинными, если на них имеется сертифицированная электронная цифровая подпись⁷.

Однако на всех документах получить такую подпись затруднительно, поэтому чаще всего судами Японии рассматриваются любые электронные доказательства, так как сложно их проверить на аутентичность. Действительно, сложность может возникнуть с использованием мультимедийной информации.

⁵ Информационные технологии в уголовном процессе зарубежных стран. Монография / Коллектив авторов; под ред. С. В. Зуева. М., 2020. 216 с. Режим доступа: Международная ассоциация содействия правосудию. URL: <http://www.iuaj.net/node/2795> (дата обращения 16.05.2021).

⁶ Христинина Е. В. Электронные доказательства в расследовании преступлений: опыт Российской Федерации и зарубежных стран // Юридический вестник

ДГУ. 2020. Т. 35, № 3. Режим доступа: Научная электронная библиотека eLIBRARY. URL: https://www.elibrary.ru/download/elibrary_44221335_36690957.pdf (дата обращения 16.05.2021).

⁷ Kaneko H. Electronic Evidence in Civil Procedure in Japan // Digital Evidence and Electronic Signature Law Review. 2008. Vol. 5. P. 211.

В Южной Корее используют «Правило лучшего доказательства» (Best Evidence Rule), когда в силу невозможности восприятия электронных документов в суде анализируются распечатки такой информации⁸.

Таким образом, в России для повышения эффективности деятельности правоохранительных органов по раскрытию и расследованию преступлений необходимо активно применять современные информационные технологии, основывающиеся на компьютерных программах, базах данных, средствах цифровой

фотографии, видео- и звукозаписи, информационных системах, информационно-телекоммуникационных сетях, а также на средствах их защиты. Современные достижения технического прогресса и их доступность допускают широкое применение различных технических средств фиксации. Значительно расширены возможности использования средств фотофиксации с помощью цифровых технологий, пришедшим на смену аналоговой фотографии, а использование видеозаписи стало легкодоступным и простым в применении.

Список литературы

1. Kaneko H. Electronic Evidence in Civil Procedure in Japan // Digital Evidence and Electronic Signature Law Review. 2008. Vol. 5. P. 211–216.
2. Информационные технологии в уголовном процессе зарубежных стран. Монография / Коллектив авторов; под ред. С. В. Зуева. М., 2020. 216 с. Режим доступа: Международная ассоциация содействия правосудию. URL: <http://www.iuaj.net/node/2795>.
3. Карлова А. В. Метод 3D-моделирования в современной судебной экспертизе // MODERN SCIENCE. 2020. №1-3. С. 81–85.
4. Христинина Е. В. Электронные доказательства в расследовании преступлений: опыт Российской Федерации и зарубежных стран // Юридический вестник ДГУ. 2020. Т. 35, № 3. Режим доступа: Научная электронная библиотека eLIBRARY. URL: https://www.elibrary.ru/download/elibrary_44221335_36690957.pdf.
5. Электронные доказательства в уголовном судопроизводстве: учебное пособие для вузов / С. В. Зуев [и др.]; ответственный редактор С. В. Зуев. Москва: Издательство Юрайт, 2021. 193 с.

⁸ Информационные технологии в уголовном процессе зарубежных стран. Монография. / Коллектив авторов; под ред. С. В. Зуева. М., 2020. 216 с. Режим доступа: Международная

ассоциация содействия правосудию. URL: <http://www.iuaj.net/node/2795> (дата обращения 16.05.2021).

Anastasia V. Karavaeva

Assistant of the Department of «Digital Forensics»,
Bauman Moscow State Technical University (National Research University)
(Moscow, Russian Federation)
karlova_av@bmstu.ru

DIGITALIZATION OF THE ACTIVITIES OF LAW ENFORCEMENT BODIES

Abstract: The article is devoted to some aspects of the use of digital technologies in the activities of law enforcement agencies. People increasingly rely on technology for their everyday needs, ranging from commerce to social interaction. For most people, technology is an integral part of everyday life. The article describes the impact of the digitalization process on the activities of law enforcement agencies, since, first of all, modern technical means should be used for the investigation, disclosure and prevention of crimes. The article also discusses aspects of the use of electronic evidence in the criminal process of the Russian Federation and foreign countries. At the moment, computerization and informatization of the activities of law enforcement agencies is of great importance. At the same time, digital technologies provide ample opportunities for the use of information resources. Based on this, the main purpose of using information technologies and computer equipment is to increase the efficiency of analysis mechanisms and the speed of information processing in order to investigate, disclose and prevent crimes.

Keywords: digitalization, law enforcement, cybercrime, digital technologies, electronic evidence, electronic evidence.

УДК: 343.13

Лучинкин Федор Михайлович

Соискатель,

Уральский государственный юридический университет

(г. Екатеринбург, Российская Федерация)

fedor-luchinkin@mail.ru

ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ОРД В ВИДЕ ЦИФРОВОЙ ИНФОРМАЦИИ В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ

Аннотация: Проблема формирования уголовно-процессуальных доказательств из результатов оперативно-розыскной деятельности является частью общей проблемы трансформации цифровой информации в письменную. В условиях цифровизации следственная технология доказывания архаична и подрывает доверие к справедливости правосудия. Электронные доказательства уравнивают стороны в доказывании и обуславливают переход к состязательной модели доказывания.

Ключевые слова: уголовный процесс, результаты оперативно-розыскной деятельности, цифровая трансформация, электронные доказательства

Для цитирования:

Лучинкин Ф. М. Использование результатов ОРД в виде цифровой информации в уголовно-процессуальном доказывании // Технологии XXI века в юриспруденции: материалы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 429–434.

Проблема использования в уголовно-процессуальном доказывании результатов оперативно-розыскной деятельности (далее – ОРД) в свете цифровой трансформации уголовного процесса привлекает все большее внимание.

Как известно по вопросу об использовании в доказывании по уголовным делам результатов ОРД есть несколько позиций.

Доминирующая позиция, которая основана на статье 89 УПК РФ, состоит в том, результаты ОРД могут быть использованы в доказывании только после их проверки следственным путем¹. Другая позиция, которую можно считать маргинальной, состоит в том, что, по крайней мере, результаты отдельных оперативно-розыскных мероприятий (далее – ОРМ): гласных ОРМ² или

¹ См.: Доля Е. А. Использование в доказывании результатов оперативно-розыскной деятельности. М.: Спарк, 1996. С. 7–8, 12; Корневский Ю. В., Токарева М. Е. Использование результатов оперативно-розыскной деятельности в доказывании по

уголовным делам: метод. пособие. М.: Юрлитинформ, 2000. С. 9, 12.

² Александров А. С., Терехин В. В., Кухта А. А. О правовом значении результатов гласных оперативно-розыскных мероприятий для уголовного дела и реформы

ОРМ, проводимых по решению суда, могут непосредственно использоваться в доказывании как в досудебном производстве, так и в судебных стадиях³. К этой позиции примыкает позиция В. В. Уткина⁴, согласно которой в судебном доказывании результаты ОРД могут быть использованы непосредственно, минуя стадию предварительного расследования. Заметим, что этот автор прямо призывает к отмене запрета, установленного статьей 89 УПК РФ.

Принципиально оппонирующий этой точке зрения А. Е. Вытовтов также вынужден был признать, что в ряде случаев сведения, полученные в ходе проведения оперативно-розыскных мероприятий, могут быть использованы в качестве средства доказывания как в предварительном расследовании, так и в суде⁵.

Представители нижегородской школы процессуалистов предлагают уравнивать результаты ОРД с результатами либо предварительного расследования (как обвинительные

досудебные доказательства), либо в качестве оправдательных доказательств – с результатами адвокатского расследования (в зависимости от обвинительного либо оправдательного характера результатов ОРД). И те, и другие досудебные доказательства, полученные сторонами до суда самостоятельно, признаются авторами равными средствами доказывания утверждений сторон в суде. Соответственно, они подлежат перекрестной двусторонней проверке в условиях состязательного судопроизводства⁶.

Несмотря на разногласия, которые имеются в науке по означенным вопросам, официальная доктрина и правоприменительная практика следуют правовому предписанию, закрепленному в статье 89 УПК РФ. Соответственно, результаты ОРД необходимо представить органу предварительного расследования в соответствии с Инструкцией⁷ с последующей легализацией этих результатов. На

досудебного уголовного процесса // Уголовное право. 2009. № 6. С. 77–81.

³ См.: Александров А. С., Кучерук Д. С. Результаты ОРМ – база приговора? Статья 1. Российский и международный опыт // Российский следователь. 2012. № 4. С. 32–35.

⁴ См.: Уткин В. В. Использование в судебном доказывании по уголовным делам результатов оперативно-розыскной деятельности: дис. ... канд. юрид. наук. Н. Новгород, 2020. С. 10.

⁵ См.: Вытовтов А. Е. Результаты оперативно-розыскной деятельности как средство доказывания в уголовном судопроизводстве (по материалам уголовных дел экономической деятельности): дис. ... канд. юрид. наук. Иркутск, 2020. С. 9.

⁶ См.: Уткин В. В. Использование в судебном доказывании по уголовным делам результатов оперативно-розыскной деятельности: дис. ... канд. юрид. наук. Н. Новгород, 2020. С. 14–15.

⁶ См.: Уткин В. В. Использование в судебном доказывании по уголовным делам результатов оперативно-розыскной деятельности: дис. ... канд. юрид. наук. Н. Новгород, 2020. С. 15.

⁶ См.: Доктринальная модель уголовно-процессуального доказательственного права РФ и Комментарии к ней / А. С. Александров [и др.]. М.: Юрлитинформ, 2015. С. 20–26.

⁷ Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ МВД России

практике это означает, как правило, проведение следственных осмотров предметов, документов, электронных носителей информации, на которых зафиксированы результаты тех или иных ОРМ. Иногда по данным материалам назначают экспертизы, а сами предметы и документы, на которых зафиксирована цифровая информация, полученная в ходе ОРД, приобщаются к уголовному делу в качестве вещественных доказательств. Хотя это условное название того носителя доказательственной информации, который преобразовался под воздействием следственной процессуальной формы.

В современной правоприменительной практике в большинстве случаев результаты ОРД имеют вид цифровой информации, представленной на электронных носителях. Поэтому в ходе следственного осмотра электронного носителя цифровой информации следователь просто фиксирует в протоколе в письменном виде часть того, что воспринял с помощью органов чувств, то есть то, что увидел и услышал. Совершенно очевидно, что это неполный и избирательный перенос информации с одного источника на другой, перевод цифровой информации в письменную. Аудио- или видеозапись хода и результатов гласных и особенно негласных ОРМ (наблюдение, прослушивание телефонных переговоров), представленная в виде цифровой информации, а тем более

результаты таких ОРМ, как снятие информации с технических каналов связи или получение компьютерной информации, должны считаться первоначальной информацией, а протоколы следственных действий, составленные на их основе – производной, то есть копией, причем копией неполной. Уже по одной этой причине понятно преимущество первичной информации, не подвергнувшейся обработке следователя, который, не будем забывать, является представителем стороны обвинения, субъектом уголовного преследования.

Перевод электронной информации в содержание письменных протоколов следственных действий – вот в чем заключается вся суть следственной проверки результатов ОРД, представленных в цифровом формате. Такова следственная технология формирования уголовно-процессуальных доказательств на основе результатов ОРД, представленных в том числе в цифровом формате. С этой технологией следователь выступает главным «трансформатором» цифровой информации в письменную. Уголовно-процессуальная система доказывания основывается на следственном стандарте или, иначе говоря, на доверии к тому, что записано в протоколе следственного действия. Критерий допустимости доказательства также в основном ориентирован на модель протокола

№ 776, Минобороны России №703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК

России № 68 от 27.09.2013 г. (зарегистрировано в Минюсте Российской Федерации 505.12.2013 г. № 30544) // Российская газета. 2013. 13 дек.

следственного действия, то есть на соблюдение требований статей 166–167 УПК РФ. На нем базируются представления о «правильном доказательстве» всех субъектов доказывания, включая судей.

Следственный уголовный процесс с присущей ему технологий доказывания основан на полномочиях следователя по формированию доказательств, то есть по фиксации полученной им информации в протоколах следственных действий и иных процессуальных документах. Следственная технология формирования доказательств основана на письменной речи, письменной речевой коммуникации и не адекватна цифровой модели коммуникации: хранения, передачи цифровой информации.

Следственная технология формирования доказательств детерминирует обвинительный уклон нашего уголовного правосудия – это главный упрек в ее адрес. То, что она не подлежит цифровой трансформации – это уже второй ее «технологический» недостаток.

В суде иногда выявляется несоответствие между содержанием протокола следственного действия и содержанием тех материалов, на основе которых он был создан следователем, то есть цифровой информации, полученной в ходе ОРД. Тогда в судебном следствии происходит непосредственный осмотр «вещественного доказательства», то есть электронного носителя информации, полученной и переданной органом, уполномоченным осуществлять ОРД, следователю. Однако такое

происходит достаточно редко. Обычно же результаты ОРД в виде цифровой информации непосредственно не исследуются, суд ограничивается оглашением протоколов следственных действий, составленных на основе результатов ОРД.

В виде исключения, при наличии спора сторон и оспаривания стороной защиты формы и содержания обвинительных доказательств, в судебном заседании воспроизводится первоисточник – носитель цифровой информации. Разумеется, для суда проще разрешить уголовно-правовой спор и ходатайство стороны защиты по протоколам следственных действий, чем обращаться непосредственно к первоисточнику – цифровой информации, которым под видом «вещественное доказательство» является материал, полученный в ходе ОРД. Судьи попали в информационную зависимость от следователей. Поэтому в изменении технологии доказывания не заинтересованы ни следователи, ни судьи, ни прокуроры.

Между тем, отказ от протокола следственного действия как эрзаца исходной доказательственной информации, полученной в ходе ОРД, не должен восприниматься как угроза системе отправления правосудия. По большинству уголовных дел спора как такого нет, в бесспорных уголовных делах, при согласии обвиняемого с обвинением, естественно, нет нужды в суде представлять и исследовать носители цифровой информации, в том числе и те, которые мы имеем в виду. Однако, если подсудимый не

признает свою вину по предъявленному обвинению, то доказательства обвинения должны быть исследованы в их первоисточниках, то есть в виде той цифровой информации, которую была получена оперативными сотрудниками при проведении ОРМ.

В современной уголовно-процессуальной науке и криминалистике часто используется понятие «электронные доказательства»⁸. При этом за редкими исключениями их отождествляют опять же со следственными доказательствами. Исключение составляют несколько работ⁹, в которых ставится методологически важный вопрос о том, что электронное доказательство не может быть только «следственным», его вполне может получить любой другой субъект с помощью технического устройства

или даже оно может быть получено машинным способом – без участия человека. При этом отпадает надобность в следственном стандарте допустимости, в протоколе следственного действия как образцовой модели источника доказательства. Доказательством может стать любая информация, представленная в любом виде субъектом доказывания в суде, если имеется возможность верифицировать ее аутентичность¹⁰.

Мы разделяем вышеуказанную позицию и считаем, что цифровая информация, полученная как оперативно-розыскным, так и следственным путем, может быть использована в суде при формировании с участием обеих сторон судебных доказательств по уголовному делу, хотя не исключается вариант и недопустимости ее в качестве средства доказывания.

Список литературы

1. Александров А. С. О правовом значении результатов гласных оперативно-розыскных мероприятий для уголовного дела и реформы досудебного уголовного процесса / А. С. Александров, В. В. Терехин, А. А. Кухта // Уголовное право. 2009. № 6. С. 77–81.

2. Александров А. С. Результаты ОРМ – база приговора? Статья 1. Российский и международный опыт / А. С. Александров, Д. С. Кучерук // Российский следователь. 2012. № 4. С. 32–35.

3. Власова С. В. К вопросу о приспособливании уголовно-процессуального механизма к цифровой реальности // Библиотека криминалиста. Научный журнал. 2018. № 1. С. 9–18.

⁸ См.: Основы теории электронных доказательств / коллектив авторов; под. ред. С. В. Зуева. М.: Юрлитинформ, 2019.

⁹ См., напр.: Пастухов П. С. Модернизация уголовно-процессуального доказывания в условиях информационного общества: дис.

... д-ра юрид. наук. М.: Московская академия экономики и права, 2015. С. 17–21.

¹⁰ См.: Власова С. В. К вопросу о приспособливании уголовно-процессуального механизма к цифровой реальности // Библиотека криминалиста. Научный журнал. 2018. № 1. С. 9–18.

4. Вытовтов А. Е. Результаты оперативно-розыскной деятельности как средство доказывания в уголовном судопроизводстве (по материалам уголовных дел экономической деятельности): дис. ... канд. юрид. наук. Иркутск, 2020. 221 с.
5. Доктринальная модель уголовно-процессуального доказательственного права РФ и Комментарии к ней / А. С. Александров [и др.]. М.: Юрлитинформ, 2015. 304 с.
6. Доля Е. А. Использование в доказывании результатов оперативно-розыскной деятельности. М.: Спарк, 1996. 111 с.
7. Корневский Ю. В. Использование результатов оперативно-розыскной деятельности в доказывании по уголовным делам: метод. пособие / Ю. В. Корневский, М. Е. Токарева. М.: Юрлитинформ, 2000. 150 с.
8. Основы теории электронных доказательств / коллектив авторов; под. ред. С. В. Зуева. М.: Юрлитинформ, 2019. 400 с.
9. Пастухов П. С. Модернизация уголовно-процессуального доказывания в условиях информационного общества: дис. ... д-ра юрид. наук. М.: Московская академия экономики и права, 2015. 454 с.
10. Уткин В.В. Использование в судебном доказывании по уголовным делам результатов оперативно-розыскной деятельности: дис. ... канд. юрид. наук. Н. Новгород, 2020. 318 с.

Fedor M. Luchinkin
Postgraduate student,
Ural State Law University
(Yekaterinburg, Russian Federation)
fedor-luchinkin@mail.ru

USE OF ORD RESULTS IN THE FORM OF DIGITAL INFORMATION IN CRIMINAL PROCEDURAL PROOF

Abstract: The problem of forming criminal procedural evidence from the results of operational-search activities is in many ways a problem of transforming digital information and writing. In the context of digitalization, the investigative technology of proof is archaic and undermines confidence in the fairness of justice. Electronic evidence equalizes the parties in evidence and determines the transition to an adversarial model of evidence.

Keywords: criminal procedure, results of operational-search activities, digital transformation, electronic evidence.

УДК 343

Доронин Максим Вячеславович

Магистрант,

Саратовская государственная юридическая академия

(г. Саратов, Российская Федерация)

maks.doronin.04@mail.ru

Научный руководитель – Г. И. Седова, кандидат юридических наук, доцент
кафедры уголовного процесс

ПРОЦЕССУАЛЬНЫЕ УСЛОВИЯ И ПРОЦЕДУРА ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация: Статья посвящена процессуальным условиям и процедуре возбуждения уголовного дела в условиях цифровизации. Отправной точкой цифровизации уголовного судопроизводства должны стать отношения, инициирующие процесс уголовного преследования. В статье выявлены проблемы отказа в возбуждении уголовного дела.

Ключевые слова: уголовный процесс, возбуждение уголовного дела, информация, цифровизация.

Для цитирования:

Доронин М. В. Процессуальные условия и процедура возбуждения уголовного дела в условиях цифровизации // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 435–439.

Актуальность темы исследования определяется тем, что одним из последствий стремительной «революции» человеческой мысли стала цифровизация, коснувшаяся в том числе и уголовного судопроизводства.

Охарактеризовать уголовно-процессуальные отношения, складывающиеся в стадии доследственной проверки, довольно сложно, по той простой причине, что у всех участников отсутствует какой-либо процессуальный статус, за исключением лица, производящего данную проверку, а также защитника,

в случае его участия в доследственной проверке.

Стадия возбуждения уголовного дела представляет собой первоначальную стадию уголовного процесса, заключающуюся в правоотношениях и деятельности ее участников при определяющей роли следователя (дознателя) по установлению наличия или отсутствия фактических и юридических оснований для начала предварительного расследования. Данная стадия включает в себя прием сообщения о преступлении, проведения по нему проверки и

принятия по итогам законного решения.

В некоторых случаях в возбуждении уголовного дела может быть отказано.

Действующее российское уголовно-процессуальное законодательство не содержит определения отказа в возбуждении уголовного дела, но анализ регулирующих данное решение норм позволяет определить его как отрицательное решение по итогам проведения проверки по сообщению¹. Отказ в возбуждении уголовного дела означает, что в силу определенных обстоятельств и условий по поводу события, о котором в уполномоченные государственные органы поступило сообщение, не может проводиться предварительное расследование.

Несмотря на подробное процессуальное регламентирование отказа в возбуждении уголовного дела, в данной области имеется и ряд проблем. Так, ч. 1 ст. 148 УПК РФ устанавливает, что отказ в возбуждении уголовного дела по п. 2 ч. 1 ст. 24 УПК РФ возможен исключительно в отношении конкретного лица. На наш взгляд, такое требование законодательства ничем не обосновано. Кроме того, в практике возникают проблемы, каким образом следует поступить, когда в совершенном деянии состав преступления очевидно отсутствует, но лицо, совершившее данное деяние, не установлено. Так, например, в случае совершения неустановленным лицом кражи имущества, которое для

владельца материальной ценности не представляет, уголовное дело возбуждено быть не может, поскольку ущерб не причинен. Принять решение об отказе в возбуждении уголовного дела по п. 1 ч. 1 ст. 24 УПК РФ будет неправильным, поскольку событие преступления имело место. В связи с изложенным представляется целесообразным исключить вышеуказанное требование из ч. 1 ст. 148 УК РФ.

Отметим, что в настоящее время в научной литературе преобладает мнение о том, что основаниями возбуждения уголовного дела являются фактические данные, относящиеся к объекту и объективной стороне преступления. Нам такое определение представляется недостаточно верным в силу его узости, так как игнорирование субъективных признаков может привести к последующему прекращению уголовного дела в связи с отсутствием состава преступления.

К примеру, наличие информации о том, что преступление могло быть совершено лицом, не достигшим возраста привлечения уголовной ответственности, по нашему мнению, должно влечь за собой производство всех возможных мероприятий по проверке истинности данной информации в рамках доследственной проверки, поскольку подтверждение такой информации является основанием для принятия решения об отказе в возбуждении уголовного дела.

¹ Ташибаева А. К. Отсутствие состава преступления – одно из оснований отказа в возбуждении уголовного дела // Право и

политика: история и современность. 2016. С. 135.

На основании изложенного, полагаем, что основанием для возбуждения уголовного дела должно признаваться наличие в деянии всех признаков состава преступления².

В то же время, статьи Особенной части УК РФ не содержат полного и подробного описания признаков состава того или иного преступления. Такое решение законодателя является верным, поскольку в ином случае нормы Особенной части УК РФ были бы неоправданно загромождены. Отсутствие подробного описания признаков состава преступления в диспозиции статей, регулирующих конкретные виды преступлений, компенсируется их раскрытием в Общей части УК РФ. Таким образом, определяя в каждом конкретном случае наличие или отсутствие состава преступления в том или ином деянии, следует анализировать нормы и Особенной, и Общей части УК РФ.

В соответствии со ст. 141 УПК РФ заявление о преступлении как основание для возбуждения уголовного дела должно представлять собой устное сообщение или письменное обращение физического лица в правоприменительный орган с информацией о совершенном, совершаемом или подготавливаемом преступлении.

Когда заявление о преступлении сделано в устной форме, то информационные технологии могут быть успешно применены для его

фиксации, регистрации, процессуального закрепления с помощью аудио- или видеозаписи, фотосъемки, компьютерных технологий, а если в письменной форме – то еще и при его доставке в правоприменительный орган посредством имеющихся телекоммуникаций.

Если заявление о преступлении сделано при производстве следственного действия, оно заносится в протокол данного следственного действия, а информационные технологии применяются (могут быть применены) в рамках определенного следственного действия в качестве альтернативных средств (аудио-и видеозапись, фотосъемка) для его фиксации, процессуального закрепления и составления необходимого процессуального документа (компьютерная и множительная техника)³.

Конкретными мерами, направленными на совершенствование уголовно-процессуального законодательства, обеспечивающими возможность более широкого использования информационно-коммуникационных технологий в уголовном судопроизводстве, с учетом вышеизложенных позиций, может стать реализация механизма межведомственного электронного взаимодействия участников

² Сверчков В. В. Соотношение понятий «состав преступления», «преступление» и «преступное посягательство» // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 7. С. 7.

³ Максимов С. В., Васин Ю. Г. Концепт инновационной модели противодействия организованной преступности: предпосылки и возможности // Всероссийский криминологический журнал. 2020. Т. 14, № 4. С. 553.

уголовного судопроизводства при направлении прокурору копий постановления руководителя следственного органа, следователя, дознавателя о возбуждении уголовного дела и об отказе в возбуждении уголовного дела, иных процессуальных документов, включая обвинительное заключение (обвинительный акт), постановление о прекращении уголовного дела, постановление о возбуждении перед прокурором ходатайства о заключении с подозреваемым или обвиняемым досудебного соглашения о сотрудничестве и др.

Межведомственное электронное взаимодействие уже доказало свою

эффективность в сфере организации предоставления государственных услуг, где успешно применяется уже около десяти лет.

Совершенствование уголовного судопроизводства за счет цифровых технологий, осуществляемое на основе приведенных принципов и по указанным направлениям, способно положительно повлиять на развитие уголовно-процессуальной формы, обеспечив ее оптимизацию при усилении гарантий правильного установления обстоятельств по уголовному делу, соблюдения прав человека, нравственных начал уголовного процесса и его воспитательного значения.

Список литературы

1. Гаврилин Ю. В. Модернизация уголовно-процессуальной формы в условиях информационного общества / Ю. В. Гаврилин, А. В. Победкин // Труды Академии управления МВД России. 2019. № 3 (51). С. 27–38.
2. Максимов С. В. Концепт инновационной модели противодействия организованной преступности: предпосылки и возможности / С. В. Максимов, Ю. Г. Васин // Всероссийский криминологический журнал. 2020. Т. 14, № 4. С. 553–569.
3. Сверчков В. В. Соотношение понятий «состав преступления», «преступление» и «преступное посягательство» // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 7. С. 7–10.
4. Ташибаева А. К. Отсутствие состава преступления – одно из оснований отказа в возбуждении уголовного дела // Право и политика: история и современность. 2016. С. 135–138.

Maxim V. Doronin

Graduate student,
Saratov State Law Academy
(Saratov, Russian Federation)
maks.doronin.04@mail.ru

Scientific supervisor – G. I. Sedova, PhD Law, Associate Professor of the Department of Criminal Process

PROCEDURAL CONDITIONS AND PROCEDURE FOR INITIATING A CRIMINAL CASE IN THE CONTEXT OF DIGITALIZATION

Abstract: The article is devoted to the procedural conditions and the procedure for initiating a criminal case in the context of digitalization. The starting point for the digitalization of criminal proceedings should be the relations that initiate the criminal prosecution process. The article reveals the problems of refusal to initiate criminal proceedings.

Keywords: criminal procedure, initiation of criminal proceedings, information, digitalization.

УДК:343

Ахметянова Виктория Эльдаровна
Студент,
Южно-Уральский Государственный Университет
(г. Челябинск, Российская Федерация)
vika3008_1999@mail.ru

Научный руководитель – Т. И. Ястребова, кандидат юридических наук, доцент
кафедры уголовного процесса, криминалистики и судебной экспертизы

ОСОБЕННОСТИ ИССЛЕДОВАНИЯ 3D-ОРУЖИЯ ПО БАЛЛИСТИЧЕСКОЙ ЭКСПЕРТИЗЕ

Аннотация: В статье рассматривается проблема того, что развитие технологических процессов приводит к неправомерному использованию технологий 3D-печати, в частности, при изготовлении огнестрельного оружия. В то же время отсутствует законодательное закрепление использования оружия, изготовленного с помощью технологий 3D-печати.

Ключевые слова: огнестрельное оружие, технологии 3D-печати, законодательное закрепление, баллистическая экспертиза, 3-D технологии.

Для цитирования:

Ахметянова В. Э. Особенности исследования 3D-оружия по баллистической экспертизе // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 440–442.

3D-принтер – это одно из самых инновационных устройств. Он предназначен для построения модели действительного объекта по сформированному на компьютере образцу трехмерной модели. 3D-принтер даёт возможность выводить объёмную информацию, создавая трёхмерные физические объекты путём их «выращивания» из полимерного материала¹.

С криминалистической точки зрения большой интерес представляет

применение технологии 3D-печати при изготовлении «гибридного» огнестрельного оружия, в котором комбинируются детали стандартных образцов стрелкового оружия и детали, напечатанные на аддитивном принтере. Наиболее известным примером подобного оружия является самозарядный пистолет Shuty-9 MP1 калибра 9x19, созданный американским плотником Дервудом. В таком случае автоматика пистолета основана на применении энергии

¹ 3D-печать оружия // 3dprofy. URL: <http://3dprofy.ru/3d-pechat-oruzhiya> (дата обращения: 10.05.2021).

отдачи свободного затвора. Такой пистолет состоит из следующих пластиковых элементов: рамки, затворной коробки, затвора, магазина ёмкостью 9 патронов и приёмника магазина².

При расследовании преступлений, связанных с использованием огнестрельного оружия, созданного путем трехмерной печати, возникает ряд криминалистических проблем. Главным вопросом для эксперта-криминалиста в таком случае будет вопрос об отнесении такого оружия к огнестрельному оружию. При решении данного вопроса будет необходимо установить такие признаки как оружейность, огнестрельность, надежность. При отсутствии какого-либо из признаков эксперт не сможет отнести оружие к огнестрельному оружию. При исследовании такого оружия нет возможности идентифицировать его по пулям и гильзам, из какого 3D-оружия они были стреляны. Однако исследователи обнаружили, что у каждого 3D-оружия есть неповторимые «отпечатки пальцев». Они представляют собой

незначительные особенности в конструкции создаваемого объекта, которые характерны исключительно для одного принтера.

3D-технологии печати открывают потенциальную возможность воссоздания отсутствующих или повреждённых деталей огнестрельного оружия промышленного производства в целях воссоздания его работоспособности. В таком случае возникает иная проблема юридической квалификации составных частей огнестрельного оружия, изготовленного путём трёхмерной печати. При проведении баллистической экспертизы будет решаться вопрос об особенностях и функциональном назначении детали оружия и её пригодности в использовании.

Огнестрельное оружие, изготовленное посредством 3D-печати, на данный момент выступает самым проблемным элементом проведения баллистической экспертизы, потому разновидности такого оружия могут не обладать обязательными признаками для признания оружия огнестрельным.

Список литературы

1. Лихачев А. С. Разъяснение некоторых положений методики установления принадлежности объекта к огнестрельному оружию / А. С. Лихачев, М. А. Сонис // Теория и практика судебной экспертизы. 2017. Том 12, № 1. С. 38–39.
2. 3D-печать оружия // 3dprofy. URL: <http://3dprofy.ru/3d-pechat-oruzhiya>.

² Лихачев А. С., Сонис М. А. Разъяснение некоторых положений методики установления принадлежности объекта к

огнестрельному оружию // Теория и практика судебной экспертизы. 2017. Том 12, № 1. С. 38–39.

Victoria E. Akhmetyanova
Student,
South Ural State University
(Chelyabinsk, Russian Federation)
vika3008_1999@mail.ru

Scientific supervisor – T. I. Yastrebova, PhD (Law), Associate Professor of the
Department of Criminal Process, Forensics and Forensic Expertise

FEATURES OF THE STUDY OF 3D WEAPONS BY BALLISTIC EXPERTISE

Abstract: The article discusses the problem that the development of technological processes leads to the illegal use of 3D printing technologies, in particular, in the manufacture of firearms. At the same time, there is no legislative consolidation of the use of weapons manufactured using 3D printing technologies.

Keywords: firearms, 3D printing technologies, legislative consolidation, ballistic expertise, 3-D technologies.

Глухов Никита Владимирович

Студент,

Елецкий государственный университет им. И. А. Бунина

(г. Елец, Российская Федерация)

gluhov.nickita2015@yandex.ru

Научный руководитель – Е. А. Очеретько, кандидат юридических наук, доцент
кафедры гражданского и предпринимательского права

РОЛЬ ЦИФРОВИЗАЦИИ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Аннотация: Стремительный рост цифровизации и существенные изменения социальной среды современного общества оказывают огромное влияние на все сферы жизни человека. Эти изменения так же влекут за собой появление новых видов преступлений, которые способствуют новым угрозам для общества. Но данные процессы также оказывают позитивное влияние на деятельность правоохранительной системы, и в первую очередь, на изменения в оперативно-розыскной деятельности. Анализу проблем и угроз, а также развитию способов борьбы правоохранительной системы с таковыми угрозами и посвящена данная статья. В работе рассмотрено влияние процесса цифровизации на уровень преступности, проанализированы новые виды преступлений, рассмотрены потенциальные возможности усовершенствования работы правоохранительной системы в борьбе с преступностью.

Ключевые слова: цифровизация, киберпреступность, оперативно-розыскная деятельность, искусственный интеллект, преступность

Для цитирования:

Глухов Н. В. Роль цифровизации в деятельности правоохранительных органов // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 443–448.

На сегодняшний день процесс роста цифровой экономики и цифровизации стремительно усилился. Эти явления оказывают огромное влияние на все сферы жизни общества и социально-экономические системы нашей страны. В силу стремительного прогресса компьютерные технологии и информационные системы стали

неотъемлемой частью нашей жизни. Такие глобальные изменения в мире естественным образом приводят к серьезным изменениям в традиционном жизненном укладе общества. Уже сегодня появились новые профессии и высокотехнологичные рабочие места, новые виды экономической деятельности, изменилось

традиционное понимание частной жизни и различные инструменты межличностного взаимодействия. И неизбежно, новый современный порядок, привел к возникновению опасных и неизвестных ранее угроз безопасности и нестабильному функционированию человеческого общества. Переход многих процессов коммуникаций и межличностных отношений в виртуальную среду, а также обширное внедрение информационных технологий в сферу бизнеса, систему государственного управления и во все гражданское общество в целом приводит к значительному росту усложнения решения проблем защиты прав и свобод человека и общества, национальных интересов государства.

В связи с этим, роль всей правоохранительной системы в целом (прокурорской, судебной, следственной деятельности и т. д.) в обеспечении безопасности граждан, а также политической, экономической, национальной безопасности государства, стремительно возросла. Для того чтобы успешно реализовать данные цели в нынешних реалиях и создать все необходимые условия для успешного социально-экономического развития страны и укрепления ее потенциала, необходимо модернизировать, улучшить и обучить правоохранительную систему в борьбе и устранении новых потенциальных угроз. Эти угрозы, возникшие в силу масштабной цифровизации практически всех сфер жизни общества, связаны с рядом изменений, обусловленных в первую очередь, растущим объемом

циркулирующей информации, а также появлением ряда проблем. Таких как обеспечение устойчивости системы государственного управления, противодействие угрозам социальной стабильности российского общества в условиях фактически открытых информационных границ, охрана государственной и коммерческой тайны, защита персональных данных, пресечение противоправных действий в информационной сфере, контроль соблюдения нормативных требований и качества услуг в информационной сфере, обеспечение бесперебойности функционирования российского сегмента глобальной сети Интернет и т. д.

В настоящее время основой становления и развития цифровой цивилизации является международная и глобальная сеть – Интернет. Она охватывают всю территорию земного шара и является связующим звеном множества региональных и локальных компьютерных сетей. Интернет – это огромная цифровая сеть, предназначенная для поиска, хранения и передачи большого количества информации. Кроме того, интернетом пользуются как наиболее быстрым и удобным способом коммуникации, поэтому в этой цифровой сети задействовано множество людей, пользующихся указанным способом коммуникации.

Одновременно с развитием электронных коммуникаций, цифровым сопровождением торговых сделок, активным внедрением технологии блокчейн и использованием криптовалюты происходит криминализация цифрового мира. Не случайно в

терминологии современных социальных и гуманитарных наук появились понятия «киберпреступление», «киберпреступность», «киберпреступник», «хакер» и другие, а в юридической теории и практике актуализируются вопросы противодействия активизировавшимся киберпреступлениям и необходимость усовершенствования цифрового права¹.

На сегодняшний день точного определения понятия «киберпреступность» не существует, но с уверенностью можно сказать, что киберпреступность – это противозаконные уголовно наказуемые деяния в сфере действия современных информационных технологий или в реальном мире с использованием данных технологий. Так называемые киберпреступления можно условно разделить на две группы. Первая группа – это преступления, связанные с взаимодействием человека и техники, а вторая группа – преступления, связанные с организованным при помощи технических средств взаимодействием человека с человеком. Причем, сегодня именно вторая группа преступлений представляет наибольшую угрозу для безопасности личности, общества и государства. Количество киберпреступлений в России растёт с

каждым днем. На сегодняшний день киберпреступления становятся все более опасными, киберпреступники представляют собой опасные объединения со своей иерархией и четкой структурой взаимодействия². Кроме того, ученые отмечают тенденцию объединения киберпреступников с организованными преступными группировками. Киберпреступность уже давно приобрела транснациональный характер, о чем неоднократно заявлялось. Например, об этом, в частности, заявлял глава Правительства РФ Д. Медведев еще в 2016 году на совещании по информационной безопасности в кредитно-финансовой сфере. Еще тогда он отметил: «По некоторым оценкам, мировые потери от киберпреступности составляют около 0,5 трлн долларов, но посчитать их очень сложно, потому что далеко не все потери фиксируются». Также Д. А. Медведев добавил, что в России число такого рода преступлений тоже растет, а опыта и сил противостоять этому явлению пока недостаточно и «бороться в одиночку с такими преступлениями практически невозможно»³.

Исходя из нынешних условий, продиктованных процессом цифровизации и определяющими настоящую реальность, для эффективной борьбы с современной преступностью необходимо

преступлениям в сфере цифровой экономики и пути их решения // Закон и право. 2018. № 3. С. 140–144.

³ Медведев: Ущерб от киберпреступности составил полтриллиона долларов // Российская газета. 2016. 3 июня.

¹ Васильев Д. В., Ласкин А. А. Проблемы правового обеспечения противодействия преступлениям в сфере цифровой экономики и пути их решения // Закон и право. 2018. № 3. С. 140–144.

² Васильев Д. В., Ласкин А. А. Проблемы правового обеспечения противодействия

модернизировать и видоизменить работу правоохранительной системы, а, в первую очередь, оперативно-розыскную деятельность. Способы и методы совершения преступлений сегодня выходят на новый уровень, преступники активно внедряют в свою противоправную деятельность новые способы и технологии, увеличивая уровень опасности своих деяний и усложняя работу правоохранительным органам. Для того чтобы успешно противостоять преступной среде, необходимо также внедрять новые методы и технологии в правоохранительной деятельности. В данной связи, самым лучшим решением на сегодняшний день представляется переход к новым упреждающим моделям организации правоохранительной деятельности, на основе внедрения технологии искусственного интеллекта (далее – ИИ).

В информационном обеспечении деятельности подразделений ОВД РФ существует потребность в обработке больших данных. Основная сложность в их обработке заключается в том, что они характеризуются многосвязной сложностью, определяемой, в том числе, необходимостью учета причинно-следственных связей на предшествующих этапах формирования информации. В правоохранительной деятельности обработка такого количества информации является необходимым условием, в целях успешного осуществления превентивной

деятельности. Именно благодаря обработке такого банка данных можно успешно определить и вычислить будущего преступника и предотвратить преступление. К сожалению, с каждым днем человеку становится все труднее обрабатывать такой объем данных. Поэтому, эффективный анализ собранных данных, а тем более предиктивная аналитика на их основе требует применения соответствующих технологий искусственного интеллекта. Технологии ИИ обладают высоким прогностическим потенциалом, а также успешностью при выборе оптимальных управленческих решений⁴. Технологии ИИ позволяют создать совершенно иные условия работы с информацией, привести в оперативно-розыскную деятельность новые возможности, учитывающие перевод в цифровую форму подавляющую часть оперативной информации. Однако, для того чтобы внедрить технологию ИИ в правоохранительную деятельность необходимо проработать ряд вопросов. Главным из них является разработка необходимого правового регулирования. Вопреки сложившемуся представлению в обществе об ИИ, данная технология обладает рядом ограничений в использовании, такими, как непрозрачность применяемых алгоритмов. Поэтому, прежде всего, совершенствование правового регулирования необходимо для того, чтобы без труда обеспечить в

⁴ Овчинский А. С., Борзунов К. К. Информация как инструмент обеспечения антикриминальной безопасности в

цифровом мире // Вестник экономической безопасности. 2019. № 3. С. 200–250.

оптимальном режиме доступ оперативных подразделений к массивам больших данных. Кроме того, для успешного внедрения данной технологии в правоохранительную деятельность, необходимо решить проблему материально технического обеспечения, обновления системы подготовки, переподготовки и повышения квалификации кадров, привлечения опыта и ресурсов бизнес-сообщества.

Важной задачей также является создание особых условий для привлечения в оперативно-розыскную деятельность квалифицированных специалистов, прошедших подготовку в области обработки данных. Кроме того, важным моментом является совершенствование методов оперативной работы, адаптации их к применению в киберпространстве и в дополненной реальности, в поиске новых методов реализации оперативно-розыскных действий и апробации их на практике. Исходя из всего вышеописанного, можно выделить основные направления для совершенствования системы информационного обеспечения МВД России. Актуальным является развитие и внедрение: технологий искусственного интеллекта, сетей передачи данных, кабельных и радиоканалов, аппаратного обеспечения для различных уровней руководства, управления и исполнителей, усовершенствованной единой системы информационно-аналитического обеспечения МВД России, информационно-аналитической системы поддержки принятия решений сотрудниками

ОВД РФ, навигационного и геопространственного обеспечения подразделений ОВД РФ.

Подводя итог сказанному выше, можно с уверенностью сказать, что в настоящее время создаются все условия для изменения и совершенствования работы правоохранительной деятельности. Процессы цифровизации неумолимо и стремительно изменяют существующий мир, затрагивая все сферы жизни общества. Вместе с этим так же трансформируется и преступность, которая активно использует имеющиеся технологии, захватывая и превращая киберпространство в свое эффективное оружие. Преступники учатся и совершенствуют свои методы с каждым днем, например, на сегодняшний день все больше участилось применение преступниками криптографических алгоритмов, существенно затрудняющих доступ к оперативно значимой информации. Поэтому внедрение новых технологий в правоохранительную деятельность представляется логичным шагом, который сможет улучшить существующие способы и методы борьбы с преступностью, а также привести новые. Стоит отметить, что на данный момент уже делаются начальные шаги к этому процессу. Поэтому данная деятельность требует дальнейшей поддержки и развития, а также заслуживает глубокого осмысления и переоценки научным сообществом, а в дальнейшем – постоянной корректировки.

Список литературы

1. Васильев Д. В. Проблемы правового обеспечения противодействия преступлениям в сфере цифровой экономики и пути их решения / Д. В. Васильев, А. А. Ласкин // Закон и право. 2018. № 3. С. 140–144.
2. Наумов В. Б. Право в эпоху цифровой трансформации: в поисках решений // Российское право: образование, практика, наука. 2018. № 6. С. 300–360.
3. Овчинский А. С. Информация как инструмент обеспечения антикриминальной безопасности в цифровом мире / А. С. Овчинский, К. К. Борзунов // Вестник экономической безопасности. 2019. № 3. С. 200–250.
4. Шестак В. А. Современные потребности правового обеспечения искусственного интеллекта: взгляд из России / В. А. Шестак, А. Г. Волеводз // Всероссийский криминологический журнал. 2019. Т. 13, № 2. С. 120–140.

Nikita V. Glukhov

Student,

Yelets State University named after I. A. Bunin

(Yelets, Russian Federation)

gluhov.nickita2015@yandex.ru

Scientific supervisor – E. A. Ocheretko, PhD (Law), Associate Professor of the
Department of Civil and Business Law

ROLE OF DIGITALIZATION IN THE ACTIVITIES OF LAW ENFORCEMENT BODIES

Abstract: The rapid growth of digitalization and significant changes in the social environment of modern society have a huge impact on all spheres of human life. These changes also entail the emergence of new types of crime that contribute to new threats to society. But these processes also have a positive impact on the activities of the law enforcement system, and first of all, on changes in the operational-search activity. This article is devoted to the analysis of problems and threats, as well as the development of ways for the law enforcement system to combat with such threats. The paper examines the impact of the digitalization process on the crime rate, analyzes new types of crimes, considers the potential for improving the work of the law enforcement system in the fight against crime.

Keywords: digitalization, cybercrime, operational-search activity, artificial intelligence.

УДК 343.98

Долгушина Полина Евгеньевна

Студент,

Московский государственный технический университет имени Н. Э. Баумана

(национальный исследовательский университет)

(г. Москва, Российская Федерация)

polina.dolgushina.18@mail.ru

Федосеева Виктория Сергеевна

Студент,

Московский государственный технический университет имени Н. Э. Баумана

(национальный исследовательский университет)

(г. Москва, Российская Федерация)

viktoriya.fedoseeva.99@mail.ru

Научный руководитель – А. В. Караваева, преподаватель

ИССЛЕДОВАНИЕ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Аннотация: В статье рассмотрено понятие вредоносного программного обеспечения, а также технических возможностей распространения вредоносного программного обеспечения. Затронуты аспекты технических возможностей распространения вредоносного программного обеспечения. В работе также отражены признаки вредоносных программ и изучены виды компьютерных вирусов по поражаемым объектам, механизму заражения, поражаемым операционным системам и платформам, дополнительной вредоносной функциональности. Рассмотрен алгоритм действий судебного эксперта при исследовании обнаруженных вредоносных программ при производстве судебной компьютерно-технической экспертизы. В ходе работы также был проведён анализ статистики уровня спама в информационно-телекоммуникационной сети Интернет, а также практический эксперимент по внедрению вредоносного файла в компьютер пользователя.

Ключевые слова: вирус, вредоносное программное обеспечение, классификация вредоносных программ, уязвимость, спам, фишинг, судебная компьютерно-техническая экспертиза.

Для цитирования:

Долгушина П. Е. Исследование вредоносного программного обеспечения: вопросы теории и практики / П. Е. Долгушина, В. С. Федосеева // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 449–455.

В последние годы, ввиду внедрения информационных технологий, появляется все больше вредоносного программного обеспечения (ВПО), которое содержит сложные механизмы защиты от обнаружения антивирусными средствами защиты.

Вредоносное программное обеспечение специально предназначено для нарушения, повреждения или получения разрешенного доступа к компьютерной системе.

Вредоносным программным обеспечением считается программное средство, созданное в целях совершения неразрешенных владельцем информации действий. При этом такими действиями могут выступать как полное уничтожение информации или системы ее защиты, так и ее блокирование, модификация либо копирование.

Одним из признаков состава преступления, предусмотренного ст. 273 УК РФ, является вредоносная программа, и согласно этой статье установлена ответственность за создание, использование и распространение вредоносных компьютерных программ.

В науке уголовного права отмечается, что квалификация преступлений, совершаемых в сфере компьютерной информации, представляет определенные трудности.

Для распространения вредоносного программного обеспечения злоумышленники используют такие эффективные техники как спам и фишинг, и тем самым мошенники выманивают

денежные средства у доверчивых получателей.

Спам – это массовая рассылка информации рекламного или иного характера людям, не дававшим своего согласия на её получение.

Фишинг представляет собой входящие на почту псевдо-уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать или обновить личные данные.

В настоящее время принято разделять следующие категории вирусов:

- по поражаемым объектам (файловые вирусы, поражающие исходный код загрузочные вирусы, соответствующие макровирусы, сценарные вирусы, просто вирусы);
- файловые вирусы делят по механизму заражения: те, которые добавляют себя в исполняемый файл, называются паразитирующими вирусами, те, которые невозможна восстановить пораженный файл, называются перезаписывающие, вирусы-«спутники» идут отдельным файлом;
- по поражаемым операционным системам и платформам (DOS, Windows, Unix, Linux, Android);
- по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
- по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);

• по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

Подробнее рассмотрим вредоносные программы:

1. Вирус (Virus, Computer virus) представляет собой самораспространяющийся вредоносный программный код, программу, активно размножающуюся путем создания и распространения своих копий, которые впоследствии могут быть модифицированы¹. Вирусы также подразделяются на загрузочные, файловые, почтовые вирусы. Такая программа содержит в себе разрушающие составные элементы, что способствует причинению значительного ущерба. Как в оперативную память, так и в дисковое пространство может проникать такой вирус и в последствии поразить разные системные файлы (например, документы), а также блокировать исправное функционирование программ.

2. Червь (Worm) является одной из форм компьютерного вируса, не осуществляющей изменение или заражение уже существующих файлов в системе, а формирующей свои собственные файлы, составляющие «тело червя». В свою очередь, черви подразделяют следующим образом: файловые черви (File worm) создают свои копии в каких-либо папках под

различными именами, присваиваемыми в произвольном порядке либо в соответствии определенным алгоритмом (например, P2P-червь).

3. Троянский конь (троянская программа либо «троянец») (Trojan horse) выступает в роли вредоносной программы, предназначенной для скрытого сбора и отправки конфиденциальных пользовательских данных, а также других ресурсов компьютера жертвы по заданным заранее злоумышленниками адресам. Зачастую такая программа создается изначально для ввода пользователя в заблуждение, т. е. использует маскировку под полезную для пользователя программу². В реальности она содержит в своей структуре деструктивные недокументированные функции, которые начинают свою деятельность только после проникновения в систему.

4. Макровирус (Macro virus) представляет собой макрос, который выполняется в автоматическом режиме и содержится в каком-либо файле документа, а также видоизменяет структуру основного используемого пользователем приложения, т. е. при формировании нового либо открытии уже существующего документа возможно присоединение к последнему макровируса, который может удалять или повреждать данные файлов,

¹ Таржанов Т. В., Кудряшов В. Е., Макарова Д. Г. Вредоносное программное обеспечение и методы борьбы с ним // Интерэкспо Гео-Сибирь. 2019. Т. 9. С. 16.

² Баюш А. А. Методические основы исследования предположительно

вредоносного программного обеспечения в рамках судебной компьютерно-технической экспертизы // Политехнический молодежный журнал. 2019. № 5 (34). С. 13.

воспроизводить визуальные эффекты, изменять настройки приложений и др.

5. Шпион (Spy) или программа-агент является вредоносной программой для несанкционированного сбора данных (пользовательских паролей и логинов). Выделяют следующие ее виды: клавиатурный шпион (KeyLogger), спуфер (Spoofing), троянский прокси (Proxy), эксплоит (Exploit); sniffер (Sniffer); руткит (Rootkit), программа удаленного администрирования (Remote access tool, Backdoor); клей (Dropper, Binder); загрузчик (Downloader); «Шутка» (Hoax, Joke); кликер (Clicker); «Звонилка» (Dialer); сканер портов (Port scanner); рекламная программа (AdWare, SpyWare); хиджакер (Hijacker).

Все вышеперечисленные виды вредоносных программ обладают следующими признаками:

1) способностью к копированию, видоизменению, уничтожению либо непосредственному блокированию определенной компьютерной информации, а также к обезвреживанию различных средств защиты последней;

2) отсутствием оповещения пользователя компьютерной информации (данных) конкретного устройства о направленности своих действий;

3) отсутствием предоставления такому пользователю выбора согласия либо несогласия на осуществление ими своих задач и цели³.

В судебно-следственной практике, пожалуй, наибольшее распространение получило признание вредоносными компьютерных программ, которые заведомо предназначены для генерации кода установки (серийного номера) и кода активации, запрашиваемых при установке лицензионных программных продуктов (KEYGEN.exe и др.).

В целом можно представить следующий алгоритм действий судебного эксперта при исследовании обнаруженных вредоносных программ при производстве судебной компьютерно-технической экспертизы, подразделяющийся на несколько стадий:

1) подготовительное исследование вредоносных программ, включающее в себя поиск и выбор антивирусного продукта, подготовку стендового компьютера (чаще всего применяются виртуальные машины, которые позволяют работать в любой гостевой операционной системе на выбор с заданными настройками параметрами);

2) непосредственное исследование вредоносных программ.

В последние десятилетия наблюдается значительный рост преступности в сфере компьютерных преступлений (компьютерных технологий), средством совершения которых служит вредоносное программное обеспечение, также называемое программным-информационным оружием и изучаемое в рамках судебной

рамках судебной компьютерно-технической экспертизы // Политехнический молодежный журнал. 2019. № 5 (34). С. 13.

³ Баюш А. А. Методические основы исследования предположительно вредоносного программного обеспечения в

компьютерно-технической экспертизы. Особенность настоящего процесса, характерная как для профессиональной, так и для социально-бытовой сферы, заключается в применении существующих методов защиты информации (ограничения доступа к ней) в целях сокрытия совершения преступления, а также методов уничтожения такой информации, способов собирания и передачи выявленных действий и непосредственно работу конкретного пользователя в сети Интернет. Эти направления заслуживают особого внимания при повышении профессионального уровня всех участников судопроизводства, в первую очередь – лиц, обладающих специальными познаниями, т. е. экспертов и специалистов, следователей.

На практическом примере можно сказать, что у пользователя файл с расширением.doc, скорее всего, не вызовет никаких подозрений, однако именно такие файлы (как.doc и.xls) очень часто используются злоумышленниками для распространения так называемых макровирусов – вредоносных скриптов, вставленных в файл как макрос. Многие не знают, что макрос, написанный на специальном языке VBA (Visual Basic for Applications), встроенный в документ Word или Excel, обладает функциями обычной программы и может использоваться в преступных целях. Чаще всего вредоносный код макроса для

получения несанкционированного доступа в операционную систему.

Для обхода почтового антивирусного детектирования вложенные файлы могут быть защищены паролем, который прилагается в письме. В открытом письме нам сообщают, что возникла неизвестная ошибка, и для ее исправления нам нужно нажать на кнопку «Enable Content». Кнопка «Enable Content» активирует код вредоносного скрипта (Макроса), содержащегося в документе. После выполнения кода на компьютер пользователя загрузится и запустится файл с названием svchost.exe, функционал которого попадает под классификацию Лаборатории Касперского Backdoor⁴.

Backdoor предназначены для удаленного управления злоумышленником пораженным компьютером. По своим функциям Backdoor во многом напоминают различные системы администрирования, разрабатываемые и распространяемые фирмами – производителями программных продуктов. Подобные вредоносные программы позволяют делать с компьютерами все, что в них заложит автор: принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и так далее.

Способных распространяться по сети и внедряться в другие компьютеры представляют особую группу под названием бэкдоров. Также внедряются в компьютеры и

⁴ Воробьев В.В. Вредоносная программа – предмет или продукт преступления? //

Государство и право в изменяющемся мире. 2016. С. 359.

сетевые черви. Отличает такие бэкдоры от червей то, что они распространяются по сети не самопроизвольно (как сетевые черви), а только по специальной команде «хозяина», управляющего данной копией троянской программы. В нашем случае вредоносный файл сохраняет свою копию в папке %Temp% и добавляет себя в автозагрузку, чтобы перезагрузка компьютера не препятствовала его работе. Затем подключается к удаленному командному серверу злоумышленника для получения дальнейших команд. Данное вредоносное программное обеспечение имеет функционал записи нажатия клавиш и последующий отправки их на сервер злоумышленника и скачивания других вредоносных файлов по ссылкам, которые содержатся в теле, по команде злоумышленника.

Эксперты Positive Technologies привели данные по количеству атак к концу 2020 года, 56 % среди всех инцидентов было использование вредоносного ПО, нацеленного на

юридических лиц. В атаках на частных лиц на первом месте находится шпионское ПО, которое составило 45 %. Больше всего операторов программ-вымогателей интересуют медицинские (20 %) и государственные учреждения (19 %), а также предприятия промышленности (11 %). Для доставки ВПО при атаках на компании злоумышленники по-прежнему используют электронную почту (65 % случаев)⁵.

Таким образом, в последние десятилетия наблюдается значительный рост преступности в сфере компьютерных технологий, средством совершения которых служит вредоносное программное обеспечение, которое характеризуется как программное обеспечение, созданное для выявления и сбора информационных данных в ЭВМ, формирования свободного доступа, использования полученной информации для причинения вреда владельцу путем искажения и несанкционированного использования ресурсов.

Список литературы

1. Баюш А. А. Методические основы исследования предположительно вредоносного программного обеспечения в рамках судебной компьютерно-технической экспертизы // Политехнический молодежный журнал. 2019. № 5 (34). С. 13.
2. Вирусы-шифровальщики представляют главную угрозу для компаний – исследование данных 2020 года // d-russia.ru. URL: <https://d-russia.ru/virusy-shifrovalshhiki-predstavljajut-glavnuju-ugrozu-dlja-kompanij-issledovanie-dannyh-2020-goda.html>

⁵ Вирусы-шифровальщики представляют главную угрозу для компаний – исследование данных 2020 года // d-russia.ru. URL: [https://d-russia.ru/virusy-shifrovalshhiki-](https://d-russia.ru/virusy-shifrovalshhiki-predstavljajut-glavnuju-ugrozu-dlja-kompanij-issledovanie-dannyh-2020-goda.html)

[predstavljajut-glavnuju-ugrozu-dlja-kompanij-issledovanie-dannyh-2020-goda.html](https://d-russia.ru/virusy-shifrovalshhiki-predstavljajut-glavnuju-ugrozu-dlja-kompanij-issledovanie-dannyh-2020-goda.html) (дата обращения: 13.04.2021).

3. Воробьев В. В. Вредоносная программа – предмет или продукт преступления? // Государство и право в изменяющемся мире. 2016. С. 357–364.

4. Дьяков Н. В. Вредоносное программное обеспечение как угроза информационной безопасности предприятий // Modern Science. 2020. № 4-1. С. 344–346.

5. Снегирев А. И. Методы распространения вредоносного программного обеспечения / А. И. Снегирев, И. Ю. Маршалова, А. Н. Вершинин [и др.] // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2019. № 1. С. 67–76.

6. Таржанов Т. В. Вредоносное программное обеспечение и методы борьбы с ним / Т. В. Таржанов, В. Е. Кудряшов, Д. Г. Макарова // Интерэкспо Гео-Сибирь. 2019. Т. 9. С. 15–18.

7. Троянский конь // SecurityLab.ru. URL: <https://www.securitylab.ru/news/212704.php>.

Polina E. Dolgushina

Student,

Bauman Moscow State Technical University (National Research University)
(Moscow, Russian Federation)
polina.dolgushina.18@mail.ru

Victoria S. Fedoseeva

Student,

Bauman Moscow State Technical University (National Research University)
(Moscow, Russian Federation)
viktoriya.fedoseeva.99@mail.ru

Scientific supervisor – A. V. Karavaeva, Lecturer

MALWARE RESEARCH: QUESTIONS OF THEORY AND PRACTICE

Abstract: The concept of malicious software is considered. The technical possibilities of spreading malicious software are considered. The article reflects the signs of malware and studies the types of computer viruses by the affected objects, by the mechanism of infection, by the affected operating systems and platforms, and by additional malicious functionality. The algorithm of actions of the forensic expert in the study of detected malware in the production of forensic computer-technical expertise is considered.

Keywords: virus, malicious software, malware classification, vulnerability, spam, phishing, forensic computer-technical expertise.

УДК 343.9

Долгушина Полина Евгеньевна

Студент,

Московский государственный технический университет имени Н. Э. Баумана

(национальный исследовательский университет)

(г. Москва, Российская Федерация)

polina.dolgushina.18@mail.ru

Федосеева Виктория Сергеевна

Студент,

Московский государственный технический университет имени Н. Э. Баумана

(национальный исследовательский университет)

(г. Москва, Российская Федерация)

viktoriya.fedoseeva.99@mail.ru

Научный руководитель – А. В. Караваева, преподаватель

ПРЕДУПРЕЖДЕНИЕ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В РФ: ИНТЕГРАТИВНЫЙ И КОМПЛЕКСНЫЙ ПОДХОДЫ

Аннотация: В настоящее время значительно повышается эффективность методов и средств проникновения преступниками в компьютерное пространство пользователей. В связи с этим очень важной становится проблема защиты данных от несанкционированного использования злоумышленниками. Растёт актуальность контроля доступа к данным и их использования. Целью данной работы является анализ способов предупреждения компьютерной преступности в Российской Федерации, а также рассмотрение киберпреступности как глобальной международной проблемы. Для достижения поставленной цели рассматриваются нормативно-правовые акты, анализ статистики уровня криминальных угроз, преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Результаты исследования показали, что обеспечение информационной безопасности является одной из важнейших задач государства в осуществлении безопасности Российской Федерации. В целях разрешения и стабилизации ситуации, связанной с компьютерной преступностью, планируется дальнейшее изучение для выстраивания взаимодействия на международном уровне в решении вопросов информационной безопасности.

Ключевые слова: компьютерная информация, безопасность данных, предупреждение преступлений, киберпреступность, криминальные угрозы, судебная компьютерно-техническая экспертиза.

Для цитирования:

Долгушина П. Е. Предупреждение компьютерной преступности в РФ: интегративный и комплексный подходы / П. Е. Долгушина, В. С. Федосеева // Технологии XXI века в

юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 456–463.

Новые информационные технологии привлекают преступников из-за огромного количества потенциальных жертв (следствие неграмотности подавляющего большинства пользователей сети Интернет в вопросах информационной безопасности), территориальной удаленности жертвы от преступника.

Компьютерная преступность представляет собой форму противоправной уголовно наказуемой деятельности, характеризующейся использованием новых информационных технологий, которые позволяют совершать преступления дистанционно, а также скрывать свою «личность» и результаты преступной деятельности путем «анонимизации» действий, при наличии временного разрыва между началом активных противоправных действий и наступлением негативных последствий. Одной из характеристик компьютерных преступлений является их «трансграничность», что значительно усложняет установление мест совершения преступлений и, следовательно, затрудняет их расследование и раскрытие¹.

Компьютерная преступность представляет собой совокупность преступлений, объектом которых являются все общественные отношения в сфере информационных

технологий и безопасного функционирования компьютерной информации. В киберпространстве могут совершаться не только преступления в сфере компьютерной информации, но и, например, доведение до самоубийства.

Комплексный подход – это использование соответствующего процесса для разбиения проблемы на элементы, необходимое для решения задачи. Каждый элемент становится меньшей и более простой задачей для представления всей системы в комплексе, т. е. осуществляется анализ системы в целом.

Интегративный подход предполагает взаимодействие, нахождение в режиме беседы, диалога с кем-либо, также предполагает обязательную непрерывность процесса обеспечения безопасности, как во времени, так и в пространстве.

Компьютерная преступность отличается высоким показателем латентности. Вызвано это рядом причин, например, нежеланием пострадавшего лица обращаться в правоохранительные органы, либо же незаметностью совершенного преступления, когда лицо даже не знает, что в отношении него оно было совершено, нежеланием сотрудников правоохранительных органов расследовать такие преступления ввиду их сложности, и многими

¹ Сафин Ф. Ю. Отдельные аспекты преступности в сфере компьютерной информации // Научная сессия ГУАП: Гуманитарные науки: сборник докладов

традиционной Научной сессии, посвященной Всемирному дню авиации и космонавтики. Санкт-Петербург, 2020. С. 221.

другими причинами. Киберпространство существует вне зависимости от границ государств. Поэтому киберпреступления могут быть трансграничными, совершаться лицами, находящимися в разных странах. Также она может носить транснациональный характер.

Преступность в области компьютерной информации приобрела характер международной, появилась острая необходимость пересмотра и повторной систематизации компьютерных преступлений². При этом требуется обязательно учитывать опыт иных государств, так как за рубежом компьютерная преступность распространена в значительно большей степени и понесенный от нее ущерб несравнимо выше.

В современном обществе информационные и коммуникационные технологии являются основным фактором, определяющим уровень социально-экономического развития и состояние национальной безопасности.

Уровень развития компьютерных технологий, скорость и объем передаваемой информации, возросшие технические возможности по ее копированию и распространению привели к росту компьютерных преступлений, посредством которых преступники осуществляют несанкционированный доступ, незаконное копирование, блокирование, модификацию и уничтожение компьютерной информации. Кроме того,

компьютерные преступления чаще становятся способом для совершения многих других умышленных преступлений, средством облегчения их совершения и уничтожения следов преступной деятельности.

Главой 28 действующего Уголовного кодекса Российской Федерации (далее – УК РФ) предусмотрена ответственность за совершение преступлений в сфере компьютерной информации. С момента принятия данного нормативного акта в 1996 г. и вступления его в силу с 01.01.1997 г. преступлениями в этой сфере считались деяния, связанные с неправомерным доступом к компьютерной информации (ст. 272 УК РФ), созданием, использованием или распространением вредоносных компьютерных программ (ст. 273 УК РФ), а также нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

Так, согласно статистическим данным, изложенным на официальном сайте Министерства внутренних дел Российской Федерации, за 2019 г. в России было зарегистрировано 2 883 преступления в сфере компьютерной информации, из которых 2 420 связаны с неправомерным доступом к компьютерной информации (ст. 272 УК РФ) и 455 – созданием, использованием и распространением вредоносных компьютерных

² Бугаев В. А., Чайка А. В. Факторы преступности в сфере компьютерных // Ученые записки Крымского федерального

университета имени В. И. Вернадского. Юридические науки. 2019. № 4. С. 140.

программ (ст. 273 УК РФ). Нетрудно посчитать, что на состав преступления, предусмотренный ст. 274 УК РФ, приходится 8 преступлений.

По оценкам аналитиков, ущерб от киберпреступности в России в 2013 г. составил 1 млрд долларов, а в 2018 г. ущерб от преступлений в сфере IT в России составил почти 400 млрд рублей. По словам директора Департамента по вопросам новых вызовов и угроз МИД России ущерб мировой экономике от преступлений в сфере информационно-коммуникационных технологий в 2019 г. возрос до 2 трлн долларов, а в 2020 г. возрастет до 3 трлн долларов.

Все это обуславливает разработку правовых норм, обеспечивающих регулирование общественных отношений, которые связаны с использованием компьютерной техники, в первую очередь – с защитой хранящейся с ее помощью информации.

Стратегические направления борьбы с преступностью в указанной сфере в нашей стране были изложены в Доктрине информационной безопасности Российской Федерации. Она представляет собой систему официальных взглядов на обеспечение национальной безопасности государства в информационной сфере, под которой понимают совокупность информации, сайтов, сетей связи, а также государственных и частных компаний, обеспечивающих их работу. Главная стратегическая цель документа – защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз,

связанных с применением информационных технологий.

Нельзя не отметить, что во многом обеспечению полноты и объективности обозначенных статистических данных способствовали проведенные в 2019 г. прокуратурами проверки достоверности отражения в документах первичного учета и базах данных информационных центров территориальных органов МВД России сведений об исследуемых преступлениях. Так, в ходе указанных проверок выявлено свыше 10 тыс. нарушений при заполнении документов первичного учета, в связи с чем принято свыше 400 мер прокурорского реагирования, в том числе внесено 161 представление, к дисциплинарной ответственности привлечено 59 должностных лиц.

В структуре преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, преобладают преступления средней тяжести (75372, или 43,2 %), далее следуют преступления небольшой тяжести (41983, или 24 %), тяжкие (37949, или 21,7 %) и особо тяжкие (19370, или 11,1 %). Значительная часть этих преступлений совершаются с использованием сети Интернет – 108016, или 61,8%, и средств мобильной связи – 61299, или 35,1 %. Остальные совершаются с использованием расчетных (пластиковых) карт – 16427 (9,4 %); компьютерной техники – 15027 (8,6 %); программных средств – 4 375

(2,5 %); фиктивных электронных платежей – 489 (0,3 %).

Уровень криминальных угроз от этих преступлений в целом по России составляет 118,9 преступлений на 100 тыс. населения страны, а уровень криминальной активности – 20,1 выявленных лиц на 100 тыс. взрослого (16 лет и старше) населения. При этом почти в 40 субъектах страны уровень криминальной активности населения больше среднего по России, причем в 10 из них этот уровень превышает средний по стране более чем в два раза. Среди них стоит отметить Республику Коми, где этот показатель превышает средний по России в три раза, и все субъекты Российской Федерации, входящие в Уральский федеральный округ.

Киберпреступность признана глобальной международной проблемой. Характерными ее особенностями являются ярко выраженный трансграничный и транснациональный характер, так как киберпространство функционирует вне рамок государственных границ и национальностей. Поэтому наибольшая трудность, стоящая перед правоохранительными органами, заключается в невозможности эффективно координировать свои действия через государственные границы, рамки различных юрисдикций и законодательных систем³.

В последние годы компьютерная преступность приобрела экономические черты, так как большинство компьютерных преступлений совершаются в

банковско-финансовом или экономическом секторе, и политическую окраску, что связано с хактивистскими движениями, а также деятельностью международных экстремистских и террористических организаций.

К специальным правовым мерам предупреждения компьютерных преступлений можно отнести следующие:

1. новации и изменения действующего уголовного законодательства, устранение пробелов;

2. по уголовным делам о компьютерных преступлениях в Российской Федерации необходимо совершенствование судебной практики;

3. в области предупреждения компьютерных преступлений нужна активизация и совершенствование международно-правового сотрудничества;

4. новации и изменения информационного законодательства РФ.

В настоящее время Министерством внутренних дел ведется разработка ряда законопроектов, призванных сформировать эффективный нормативно-правовой механизм реализации государственной политики в области обеспечения информационной безопасности в целом и борьбы с информационной преступностью в частности. Регулярно проводятся конференции, совещания и семинары, посвященные данной проблематике.

³ Халиуллина Э. Т. Криминогенные факторы компьютерной преступности в России //

Вестник Академии Следственного комитета Российской Федерации. 2019. № 4 (22). С. 57.

Общэкономические превентивные меры включают: повышение конкурентоспособности национальной экономики; экономический рост, который достигается, прежде всего, путем развития национальной инновационной системы и инвестиций в человеческий капитал; повышение производительности труда и др.

Организационные меры основываются на подборе кадров или проверке персонала, который имеет прямое отношение к информационным базам, и в связи с этим доступ к ним нужно ограничивать. Наличие прав работы с информацией у людей с сомнительным прошлым или относящихся к работе небрежно может привести к утечкам данных.

Технические меры делятся на две группы: аппаратные и программные.

Аппаратные меры включают в себя наличие технических устройств, обеспечивающих защиту, а именно: средства охранно-пожарной сигнализации, современные устройства экранирования аппаратуры и соответственных линий проводной связи, инновационные устройства защиты телефонии от прослушивания, источники бесперебойного питания, оберегающие от скачков напряжения.

К программным мерам предупреждения компьютерной преступности относят антивирусную защиту, позволяющую осуществлять охрану компьютеров от внедрения вредоносного программного обеспечения. Достаточно высокий уровень защиты от различных вирусных программ предоставляют собой современные антивирусные программы. Антивирусные программы в целом могут распознавать нежелательные действия со стороны вредоносного носителя.

Таким образом, обеспечение информационной безопасности стало одной из важнейших задач государства в контексте современной стратегии национальной безопасности Российской Федерации, в том числе и вследствие появления транснациональной компьютерной преступности и угрозы кибертерроризма. С учетом того, что информационное пространство фактически превращается в «арену противостояния», особое значение приобретает международно-правовое регулирование правоотношений в сети Интернет. Необходимо выстраивать взаимодействие на международном уровне в решении вопросов информационной безопасности, которые, по оценкам экспертов, являются ключевым элементом системы коллективной безопасности.

Список литературы

1. Бугаев В. А. Факторы преступности в сфере компьютерных технологий / В. А. Бугаев, А. В. Чайка // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2019. № 4. С. 139–145.

2. Лазарева К. А. Актуальные вопросы противодействия компьютерной преступности в Российской Федерации / К. А. Лазарева, Е. С. Серогодская // Юридический факт. 2020. № 82. С. 16–18.

3. Лахтиков Д. Н. Теория и практика борьбы с компьютерной преступностью. Минск: Академия МВД, 2020. 112 с.

4. Сафин Ф. Ю. Отдельные аспекты преступности в сфере компьютерной информации // Научная сессия ГУАП: Гуманитарные науки: сборник докладов традиционной Научной сессии, посвященной Всемирному дню авиации и космонавтики. Санкт-Петербург, 2020. С. 221–222.

5. Халиуллина Э. Т. Криминогенные факторы компьютерной преступности в России // Вестник Академии Следственного комитета Российской Федерации. 2019. № 4 (22). С. 55–59.

Polina E. Dolgushina

Student,

Bauman Moscow State Technical University (National Research University)

(Moscow, Russian Federation)

polina.dolgushina.18@mail.ru

Victoria S. Fedoseeva

Student,

Bauman Moscow State Technical University (National Research University)

(Moscow, Russian Federation)

viktoriya.fedoseeva.99@mail.ru

Scientific supervisor – A. V. Karavaeva, Lecturer

COMPUTER CRIME PREVENTION IN THE RUSSIAN FEDERATION: INTEGRATIVE AND INTEGRATED APPROACHES

Abstract: The methods and means of penetration by criminals into the computer space of users are significantly increasing at the moment. In this regard, the problem of protecting data becomes very important from unauthorized using by intruders. The importance of controlling access to and use of data is growing. The purpose of this paper is to analyze the ways of preventing computer crime in the Russian Federation, as well as to consider cybercrime as a global international problem. In order to achieve this goal, we consider regulatory legal acts, analysis of statistics on the level of criminal threats, crimes committed using information and telecommunications technologies or in the field of computer information. The results of the study showed that ensuring information security is one of the most important tasks of the state in the implementation of the security of Russian Federation. We plan to study further to build cooperation at the international level in addressing issues of information security, in order to resolve and stabilize the situation related to computer crime.

Keywords: computer information, data security, crime prevention, cybercrime, criminal threats, forensic computer and technical expertise.

Зиновенкова Алёна Андреевна

Студент,

Южно-Уральский Государственный Университет

(г. Челябинск, Российская Федерация)

al_zinovenkova@mail.ru

Сутягин Владимир Сергеевич

Студент,

Южно-Уральский Государственный Университет

(г. Челябинск, Российская Федерация)

vladimirsut555@mail.ru

Научный руководитель – Т. И. Ястребова, кандидат юридических наук, доцент
кафедры уголовного процесса, криминалистики и судебной экспертизы

ОТДЕЛЬНЫЕ АСПЕКТЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация: В статье рассмотрены вопросы тактики расследований преступлений в сфере компьютерной информации. В частности, затронут аспект следственных действий, проводимых правоохранительными органами с учётом современных цифровых технологий. Кроме того, затронут вопрос сложности квалификации данных преступлений.

Ключевые слова: компьютерная информация, расследование преступлений, эксперт, специалист, уголовный процесс.

Для цитирования:

Зиновенкова А. А. Отдельные аспекты расследования преступлений в сфере компьютерной информации / А. А. Зиновенкова, В. С. Сутягин // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 464–467.

С появлением IT-технологий все чаще совершаются преступления в сфере компьютерной информации. Так, в январе 2020 года зарегистрировано 28,1 тыс. преступлений, совершённых с использованием информационно-

телекоммуникационных технологий или в сфере компьютерной информации, что на 75,2 % больше, чем за аналогичный период прошлого года¹. Из приведенной статистики можно сказать, что тенденция

¹ Краткая характеристика состояния преступности в Российской Федерации за 2020 год // Официальный сайт МВД РФ.

URL: <https://xn--b1aew.xn--plai/reports/item/19655871/> (дата обращения: 15.03.2021).

совершения преступлений увеличивается с каждым периодом.

К преступлениям в сфере компьютерной информации относят четыре вида преступлений. Данные преступления отражены в главе 28 УК РФ, в том числе:

1. Незаконное использование и доступ к информационному ресурсу; Разработка, использование, распространение и внедрение вирусных электронных программ.

2. Нарушения в области хранения, передачи и обработки информационных потоков.

3. Незаконные действия с целью причинения вреда критической информационной системе и структуре РФ.

Сложность в расследовании преступлений данной группы заключается в первую очередь в их квалификации, поскольку следственные органы должны обладать специальными знаниями в области электронных технологий. Специалисты следственных органов к тому же должны обладать знаниями о способах и возможностях, связанных с запрещенным внедрением в интернет-сеть, копированием, нарушением способов хранения информации, взломом систем, разработкой, внедрением специальных программ. Так, следственные органы должны правильно изымать компьютерную информацию, обеспечить ее сохранность и оградить от посторонних лиц данную изымаемую информацию, поскольку возможны попытки плагиата. Не производить каких-либо манипуляций до правильного изъятия данной компьютерной информации. Как

правило, таким вопросам особое внимание уделяется специалистами, которые занимаются защитой информации от несанкционированного доступа, так как именно они, как правило, самостоятельно «пишут» программы, направленные на защиту информации и знают все их слабые и сильные стороны.

Таких сотрудников, как правило, в правоохранительных органах мало и следователям самим приходится справляться с подобными ситуациями в данной сфере преступлений.

Определенные вопросы возникают и к положениям, связанным с регулированием процесса доказывания по уголовным делам указанной категории.

Информация, интересующая следствие, которая изымается из рабочего компьютерного устройства или сети, динамична, идентифицировать ее можно лишь по ее цифровому следу, который можно прочесть благодаря хэш-сумме компьютерной информации, вычисляемой различными способами. Обычно информация изымается на какой-либо носитель (флэш-накопитель, диск), но может изыматься и в виде цифрового следа. Такой вид доказательства как цифровой след, в ч. 2 ст. 74 УПК РФ не предусмотрен, соответственно не разработан конкретный механизм получения такого вида доказательства и порядок работы с ним, в то время как при расследовании преступлений, совершенных с использованием компьютерных технологий, информация, получаемая с таких

цифровых следов, является наиболее значимой, поскольку она обладает таким признаком, как высокая скорость трансформации.

Думается, что именно методология такой науки как «форензика» способна разработать соответствующий порядок работы с цифровыми следами совершения преступлений². Данная проблема, несомненно, нуждается в разрешении.

Еще один аспект проблемы, на котором мы хотели бы заострить внимание, это участие понятых при проведении следственных действий касемо преступлений в сфере компьютерной информации. Понятой по правилам должен быть способен полно и правильно воспринимать сущность действий, происходящие в его присутствии и осознанно подтвердить своей подписью содержание процесса следственного действия, что вряд ли достижимо, учитывая то, какая категория уголовных дел расследуется. А это значит, что прежде чем проводить следственные действия по преступлениям рассматриваемой категории, следователю необходимо продумать организационные варианты приглашения граждан к участию в следственных действиях по уголовным делам, расследуемым в сфере компьютерной информации, а это весьма сложная задача, имеющая к тому же определенные, порой не оправданные, риски.

Сегодня особую важность при производстве следствия по уголовным делам о преступлениях, как рассматриваемой категории дел, так и всех иных, приобретает вопрос цифровизации производства по уголовному делу, причем полной его цифровизации, а не отдельных элементов.

Таким образом, для правильного расследования и раскрытия преступлений в сфере компьютерной информации предлагаем:

1. Издать специальную инструкцию, которая позволит эффективно разбираться в особенностях данного вида преступлений, и даст криминалистический анализ данных деяний, как это в свое время было сделано для других видов преступлений.

2. Внести в перечень видов доказательств новый вид доказательства – цифровой след, предусмотрев также порядок его процессуального обнаружения, изъятия и закрепления.

3. Внести дополнения в ч. 3 ст. 170 УПК РФ, связанные с исключением участия понятых в следственных действиях в рамках производства по делам об ИТ-преступлениях, обязав сотрудников правоохранительных органов проводить только видеофиксацию проводимых следственных действий.

4. Цифровизация производства позволит значительно облегчить

² Бунин К. А. Особенности осуществления ОРМ «Получение компьютерной информации» и его отграничение от схожих ОРМ // Уголовный закон: современное состояние и перспективы развития:

материалы II Международной научно-практической конференции, приуроченной ко дню принятия Уголовного кодекса РФ (Воронеж, 24 мая 2016 г.). Воронеж: АМиСта, 2018.

процесс как в аспекте заполнения постановлений, так и в их хранении, необходимых протоколов и исследовании.

Список литературы

1. Кузнецов П. С. Проблемы расследования преступлений в сфере компьютерной информации // Молодой ученый. 2020. № 15 (305). С. 210–212.
2. Развитие информационных технологий в уголовном судопроизводстве: монография / под ред. С. В. Зуева. М.: Юрлитинформ, 2018. 248 с.

Alena A. Zinovenkova
Student,
South Ural State University
(Chelyabinsk, Russian Federation)
al_zinovenkova@mail.ru

Vladimir S. Sutyagin
Student,
South Ural State University
(Chelyabinsk, Russian Federation)
vladimirsut555@mail.ru

Scientific supervisor – T. I. Yastrebova, PhD (Law), Associate Professor of the
Department of Criminal Process, Forensics and Forensic Expertise

CERTAIN ASPECTS OF THE INVESTIGATION OF CRIMES IN THE FIELD OF COMPUTER INFORMATION

Abstract: The article deals with the tactics of investigating crimes in the field of computer information. In particular, the aspect of investigative actions carried out by law enforcement agencies will be touched upon, taking into account modern digital technologies. The issue of the complexity of the qualification of these crimes will be raised.

Keywords: computer information, crime investigation, expert, specialist, criminal procedure.

Зунгруев Аюка Витальевич

Курсант,

Ленинградский областной филиал

Санкт-Петербургского университета МВД России

(Ленинградская область, г. Мурино, Российская Федерация)

aveter254@gmail.com

Медведев Виталий Александрович

Преподаватель кафедры социально-экономических

и гуманитарных дисциплин,

Ленинградский областной филиал

Санкт-Петербургского университета МВД России

(Ленинградская область, г. Мурино, Российская Федерация)

smit-vint@yandex.ru

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Аннотация: В статье рассматриваются примеры использования информационных технологий для пресечения и противодействия преступлениям. В наши дни практика использования новых компьютерных методов в большей степени распространяется на криминалистику. В связи с этим возникают вопросы, связанные с использованием средств информационных технологий при раскрытии и расследовании преступлений.

Ключевые слова: преступление, портрет преступника, автоматизированные информационные системы, габитоскопия, криминалистика.

Для цитирования:

Зунгруев А. В. Использование информационных технологий в раскрытии и расследовании преступлений / А. В. Зунгруев, В. А. Медведев // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 468–471.

В XXI веке перед правоохранительными органами открывается огромный простор по использованию средств для раскрытия преступлений. Появление новых средств и методов раскрытия и расследования преступлений обусловлено развитием информационных технологий, а

именно компьютеризацией и информатизацией общества. Этот процесс был запущен в 90-х годах, когда интернет получил свое активное развитие и распространение по всему миру. Именно тогда начала развиваться киберпреступность и именно тогда были придуманы новые средства и методы по борьбе с ней.

Появление информационной преступности несомненно способствовало активному развитию инновационных средств и методов по борьбе с ней. С помощью новоизобретенных методов стали расследовать и «обычные» преступления, не связанные с информационной преступностью. Также стоит отметить, что процесс информатизации общества значительно облегчил деятельность правоохранительных органов и в повседневной их работе, например, в работе с документацией. Ведь с появлением и развитием компьютеров появились и различного рода программы, позволяющие быстро составлять, изменять и обрабатывать документы, а также вести учет, составлять статистику и многое другое.

В наши дни практика использования новых компьютерных методов в большей степени распространяется на криминалистику. В этой области существуют программы, позволяющие моделировать образ преступника с учетом его специфических черт. Использование данных программ является достаточно перспективным направлением развития. Однако, необходимо заметить, что наличие современных автоматизированных информационных систем в подразделениях ОВД не обеспечивает высокий уровень раскрытия преступлений. Важным условием достижения положительного эффекта является правильное и своевременное

их применение, поскольку на сегодняшний день алгоритм раскрытия преступления является устаревшим. Даже схема построения образа преступника сопровождается долгими рутинными поисками по карточкам и базам данных. Нужно перестраивать установившуюся систему и активно использовать новоизобретенные информационные методы и средства, которые значительно сократят время на оперативно-следственные мероприятия и увеличат время на принятие решений для розыска и задержания подозреваемого.

Сейчас видится необходимым подробнее описать алгоритм работы составления модели преступления и поиска подозреваемых лиц с помощью специальной программы «Форвер»¹. В программу «Форвер» заносятся все необходимые признаки преступления, например, такие как:

1. Место убийства;
2. Пол и возраст жертвы;
3. Способ совершения убийства и т. д.

На основании введенных нами данных, программа находит аналогичные дела, в которых нас интересуют признаки лиц, совершивших убийство. Использование данной программы заключается в том, что мы вводим в нее известные нам признаки преступления, для эффективной работы желательно не менее шести признаков. После того как мы ввели все необходимые признаки программа автоматически ищет похожие дела по

¹ Платонов В. А. Использование информационных технологий в раскрытии и расследовании преступлений // Проблемы

современной науки и образования. 2017. С. 52–54.

базам данным субъекта. И выдает результат. Также на основании полученной информации составляется портрет преступника. Хочется отметить, что эффективность работы данной программы зависит от базы данных, имеющейся в субъекте, то есть будет не эффективно использовать данную программу в Ростове, если преступление произошло в Туле.

Также существуют специальные программы, модули, которые сами формируют компьютерную модель, портрет злоумышленника. Алгоритм данных программ состоит из следующих этапов²:

1. Составление словесного портрета.
2. Составление субъективного портрета злоумышленника.
3. Работа с модулем габитоскопии.
4. Поиск подозреваемых лиц.
5. Отчет.
6. Корректировка составленного портрета.

Получение всей необходимой информации о преступнике происходит в первых двух этапах, после этого специалист оценивает достоверность полученной информации и переходит к работе с

модулем габитоскопии. На четвертом этапе происходит сортировка изображений по степени схожести с составленным портретом. После того как получены результаты поиска подозреваемых они переходят в распоряжение специалистов, ведущих розыск. И на основании полученных результатов они уже могут устанавливать личность подозреваемого. Последний этап является факультативным. В случае не нахождения в базе данных лица, подходящего под описание, необходимо произвести корректировку словесного и субъективного портрета.

Таким образом, появление новых программ, методов и средств в сфере расследования и раскрытия преступлений значительно облегчают процесс пресечения и противодействия преступлениям, а также помогают более оперативно действовать сотрудникам правоохранительных органов. Внедрение новых технологий является перспективным направлением развития, которое поможет снизить уровень преступности и повысить процент раскрываемости совершаемых преступлений в будущем.

Список литературы

1. Демина Р. Е. Совершенствование организации и использования криминалистических учетов МВД России для успешного раскрытия преступлений // Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2019. № 2 (14). С. 44–47.

² Ковалев С. А., Смагоринский Б. П. Использование криминалистического компьютерного моделирования при

планировании расследования преступлений // Юридическая наука и правоохранительная практика. 2013. С. 111–123.

2. Ковалев С. А. Использование криминалистического компьютерного моделирования при планировании расследования преступлений / С. А. Ковалев, Б. П. Смагоринский // Юридическая наука и правоохранительная практика. 2013. С. 111–123.

3. Малюгина А. В. Возможности оптимизации и совершенствования деятельности полиции России, связанные с применением технологических инноваций (анализ зарубежного опыта) / А. В. Малюгина, А. Н. Ануфриева // European Journal of Natural History. 2020. № 4. С. 78–84.

4. Платонов В. А. Использование информационных технологий в раскрытии и расследовании преступлений // Проблемы современной науки и образования. 2017. С. 52–54.

5. Рак И. П. Информационные технологии в деятельности правоохранительных органов // Инновационная наука. 2016. № 2-3. С. 132–135.

Ayuka V. Zungruev

Cadet,

Leningrad regional branch

St. Petersburg University of the Ministry of Internal Affairs of Russia

(Leningrad region, Murino, Russian Federation)

aveter254@gmail.com

Vitaly A. Medvedev

Lecturer of the Department of Socio-economic and Humanitarian Disciplines,

Leningrad Regional branch

St. Petersburg University of the Ministry of Internal Affairs of Russia

(Leningrad region, Murino, Russian Federation)

smit-vint@yandex.ru

THE USE OF INFORMATION TECHNOLOGIES IN THE DETECTION AND INVESTIGATION OF CRIMES

Abstract: The article considers examples of the use of information technologies for the suppression and counteraction of crimes. Nowadays, the practice of using new computer methods is more extended to criminology. In this regard, there are questions related to the use of information technology tools in the detection and investigation of crimes.

Keywords: crime, criminal portrait, automated information systems, habitoscopy, criminalistics.

УДК 34

Капканникова Марина Алексеевна

Студент,

Саратовская государственная юридическая академия

(г. Саратов, Российская Федерация)

kapkannikova.marina@bk.ru

Кочетова Елена Евгеньевна

Студент,

Саратовская государственная юридическая академия

(г. Саратов, Российская Федерация)

kochetova.elenaa@yandex.ru

Анисимова Алина Сергеевна

Кандидат юридических наук, старший преподаватель кафедры информационного права и цифровых технологий,

Саратовская государственная юридическая академия

(г. Саратов, Российская Федерация)

saninp@rambler.ru

КИБЕРПРЕСТУПНОСТЬ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ: МАСШТАБЫ, РИСКИ И МЕТОДЫ БОРЬБЫ

Аннотация: В статье рассматривается такое явление как киберпреступность, указаны и проанализированы его масштабы, а также предложены меры, которые можно использовать в борьбе с ним. Затрагивается вопрос использования в информационных системах биометрических систем с точки зрения обеспечения информационной безопасности. Выделены риски, которые могут возникнуть в результате использования биометрических систем, и обозначены рекомендации по предотвращению подобных рисков.

Ключевые слова: киберпреступность, информационное общество, биометрическая система, биометрические данные, персональные данные, информационные технологии, киберпреступники, Интернет.

Для цитирования:

Капканникова М. А. Киберпреступность в современном информационном обществе: масштабы, риски и методы борьбы / М. А. Капканникова, Е. Е. Кочетова, А. С. Анисимова // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 472–477.

Современное общество пребывает на том уровне развития, когда компьютеры и телекоммуникационные системы охватывают все сферы жизнедеятельности человечества. Без указанных средств уже не представляется возможным нормальное функционирование общества в целом. Однако, внедрив данные системы в свою жизнь, человечество не предусмотрело вытекающие последствия, то, к чему может привести такое развитие. На сегодняшний день жертвами преступников, осуществляющих незаконную деятельность в виртуальном пространстве, могут стать как люди, так и целые государства. Количество преступлений, совершаемых в киберпространстве, увеличивается пропорционально числу пользователей компьютерных сетей. Киберпреступность – это глобальная опасность не только для России, но и для всего мира в целом.

Киберпреступность – это следствие глобализации информационно-коммуникационных технологий и появления международных компьютерных сетей. В отличие от других видов экономической преступности, киберпреступность в настоящее время является наиболее быстрорастущим сегментом, что связано с увеличением

численности пользователей компьютеров, подключенных к глобальной сети Интернет, постоянным повышением уровня профессионализма киберпреступников, устойчивым развитием и совершенствованием информационных технологий¹.

К 2023 году доля киберпреступлений может вырасти с 14 до 30 %, прогнозируют аналитики организации «Интернет-розыск». Это связано с низкой раскрываемостью и слабыми возможностями по идентификации онлайн-злоумышленников². «В 2019 году в России потери экономики от киберпреступлений составили 2,5 трлн руб., по итогам 2020 года эта цифра может увеличиться еще на 1 трлн руб. при условии, если мы не будем принимать экстренных мер по борьбе с киберпреступностью», – заявил заместитель председателя правления Сбербанка Станислав Кузнецов. При этом он отметил, что в связи с пандемией коронавируса в 2021 году потери от киберпреступности продолжат увеличиваться³. Именно поэтому в целях защиты от хакерских атак в экономически развитых странах значительно увеличиваются затраты на кибербезопасность.

Исходя из основных положений киберпреступности, необходимо отметить биометрическую систему

¹ Гундериц Г. А. Состояние киберпреступности // Научный вестник Крыма. 2018. № 4 (15).

² Сидоренко Е. По цифровым следам: в РФ раскрывается лишь четверть киберпреступлений // Известия. 2020. 13 янв. URL: <https://iz.ru/962966/elena-sidorenko/po-tcifrovym-sledam-v-rf-raskryvaetsia-lish->

chetvert-kiberprestuplenii (дата обращения: 10.03.2021).

³ Сбербанк: Потери российской экономики от киберпреступлений могут составить 3,5 трлн руб. по итогам года // Рамблер: Финансы. 2020. 18 июня. URL: <https://finance.rambler.ru/markets/44370484> (дата обращения: 10.03.2021).

как новый способ доступа к информации. Так, для контроля доступа к информационным системам далеко не последнюю роль играют процессы идентификации и аутентификации пользователей, которые позволяют определить пользователя по идентификатору и проверить его подлинность. Известно, что в этом случае данные системы основаны на связке логина и пароля, где пользователь запоминает эту комбинацию и использует ее для пользования информацией.

В последние годы набирают популярность системы, которые используют биометрические данные человека. Простота и удобство в пользовании такими системами заключается в том, что данные находятся всегда с человеком, ему не нужно ничего дополнительно запоминать или удостоверять свою личность при помощи каких-либо документов. Среди плюсов можно также выделить отсутствие риска потери или забывания указанных данных.

Биометрические системы и принципы их функционирования основываются на науке о биометрии и биометрических данных. Под наукой о биометрии подразумеваются способы автоматизированного распознавания человека по уникальным физическим и (или) психологическим признакам, которые присущи только одной

конкретной личности. Опираясь на межгосударственный стандарт, можно понять, что выделяют два ключевых понятия в данной сфере: биометрическую идентификацию (или, по-другому, распознавание) и аутентификацию (она же – верификация), и эти понятия, как может показаться на первый взгляд, далеко не одно и то же⁴.

Под биометрической идентификацией (распознаванием) понимается база данных, где хранятся все полученные образцы какого-либо признака всех индивидов, для которых требуется предоставить доступ, и при сравнении с каждым из которых можно определить, является ли заявитель тем, чей признак есть в базе, или нет. Биометрическая аутентификация (верификация) представляет собой сам процесс сравнения признака из базы данных с предъявляемым для подтверждения истинности и принятия соответствующего решения о предоставлении доступа к информационным системам⁵.

Технологии распознавания набирают популярность не только на российском рынке, но и за рубежом. Так, разработчики продукции Apple используют TouchID и FaceID, Microsoft – WindowsHello. Биометрические датчики присутствуют в комплектации

⁴ ГОСТ ISO/IEC 2382-37-2016 Информационные технологии (ИТ). Словарь. Часть 37. Биометрия: национальный стандарт Российской Федерации: введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 февраля 2017 г. № 71-ст: дата введения 2017-07-01.

М.: Стандартиформ, 2018 год. Режим доступа: Электронный фонд правовых и нормативно-технических документов. URL: <http://docs.cntd.ru/document/1200144206> (дата обращения: 10.03.2021).

⁵ Чурилин Г. Н., Максимова Е. А. Биометрия в информационной безопасности // NBI-technologies. 2019. № 4.

большого числа новых моделей смартфонов, планшетов и ноутбуков.

Если говорить о более серьезных отраслях и сегментах, таких как банки и бизнес-системы, то биометрия начинает успешно внедряться и там. Начиная с лета 2018 года, в России заработала Единая Биометрическая Система (далее – ЕБС), оператором которой является «Ростелеком», и которая уже используется некоторыми крупными банками Российской Федерации⁶.

В мире не существует абсолютно неуязвимых технологий, и в результате использования биометрических систем появляются определенные риски. Так, при сборе биометрических данных может возникнуть угроза нарушения их целостности (например, в случае удаления или подмены биометрических персональных данных сотрудниками, занимающимися их сбором и занесением в систему). В случае раскрытия и (или) передачи данных третьим лицам может возникнуть угроза нарушения их конфиденциальности. Следует также выделить риски, связанные с нарушениями при неправильной обработке или хранении биометрических персональных данных, или в случае успешной подделки злоумышленником образцов

биометрического материала в ходе биометрической верификации.

В целях предотвращения подобных рисков рассмотрим рекомендации, предоставленные Центральным банком Российской Федерации вследствие введения системы ЕБС:

1) Рекомендуется использовать средства криптографической защиты информации (СЗКИ), имеющие подтверждение требований надежности.

2) Рекомендуется размещать объекты, связанные с обработкой биометрических персональных данных, в отдельных сегментах вычислительных сетей. Доступ к отдельному сегменту проще контролировать, а значит, лица, не имеющие на то доступ, легко его не получат.

3) Рекомендуется уведомить сотрудника, занимающегося обработкой и сбором биометрических данных, о протоколировании его действий, а также об ответственности за нарушение законодательства РФ в данной сфере⁷.

Как уже было ранее сказано, не существует систем, которые не могли бы быть полностью неуязвимыми и абсолютными. Одним из векторов защиты от нарушения информационной безопасности может являться соблюдение законодательства информационной

⁶ ЦБ решил обязать банки оказывать услуги с использованием биометрии клиентов. // Интерфакс. 2019. 24 мая. URL: <https://www.interfax.ru/business/662298> (дата обращения: 10.03.2021).

⁷ Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и

хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации // Центральный банк: официальный сайт. URL: <http://www.cbr.ru/content/document/file/62907/4mr.pdf> (дата обращения: 10.03.2021).

безопасности (далее – ИБ) в данной сфере. Первым делом стоит понимать, что биометрические признаки всех групп относятся к персональным данным.

Проанализировав и разобрав основные аспекты таких нововведений в наше быстроразвивающееся общество, хотелось бы отметить, что биометрические системы выступают в качестве удобных систем идентификации пользователей. Хранение биометрических образцов требует обеспечения крайне высокого уровня защиты, и на данном этапе развития сложно сказать, являются ли указанные данные более надежными, чем «традиционные».

Для борьбы с киберпреступностью в современном информационном обществе необходимо принять следующие меры:

- более ответственно и качественно подойти к этому вопросу уполномоченным органам и

должностным лицам, следить за соблюдением законодательства в сфере ИБ и принимать надлежащие меры в случае его нарушения;

- разъяснять сотрудникам, работающим в сфере сбора и обработки биометрических данных, их права и обязанности и предупреждать об ответственности за возможные нарушения;

- принимать меры в сфере оптимизации законодательства под непосредственно возникающие угрозы и нарушения в сфере ИБ;

- увеличить затраты федерального бюджета на повышение уровня кибербезопасности;

- проанализировать зарубежный опыт борьбы с киберпреступностью и внедрить наиболее успешные технологии в нашем государстве;

- принимать меры по увеличению числа высококлассных специалистов по информационной безопасности в России.

Список литературы

1. Гундерич Г. А. Состояние киберпреступности // Научный вестник Крыма. 2018. № 4 (15).
2. Сбербанк: Потери российской экономики от киберпреступлений могут составить 3,5 трлн руб. по итогам года // Рамблер: Финансы. 2020. 18 июня. URL: <https://finance.rambler.ru/markets/44370484>.
3. Сидоренко Е. По цифровым следам: в РФ раскрывается лишь четверть киберпреступлений // Известия. 2020. 13 янв. URL: <https://iz.ru/962966/elena-sidorenko/po-tcifrovym-sledam-v-rf-raskryvaetsia-lish-chetvert-kiberprestuplenii>.
4. ЦБ решил обязать банки оказывать услуги с использованием биометрии клиентов // Интерфакс. 2019. 24 мая. URL: <https://www.interfax.ru/business/662298>.
5. Чурилин Г. Н. Биометрия в информационной безопасности / Г. Н. Чурилин, Е. А. Максимова // NBI-technologies. 2019. № 4. С. 30–36.

Marina A. Kapkannikova

Student,
Saratov State Law Academy
(Saratov, Russian Federation)
kapkannikova.marina@bk.ru

Elena E. Kochetova

Student,
Saratov State Law Academy
(Saratov, Russian Federation)
kochetova.elenaa@yandex.ru

Alina S. Anisimova

PhD (Law), Senior Lecturer of the Department of Information Law and Digital
Technologies,
Saratov State Law Academy
(Saratov, Russian Federation)
saninp@rambler.ru

CYBERCRIME IN THE MODERN INFORMATION SOCIETY: SCALE, RISKS AND METHODS OF METHODS OF COMBATING

Abstract: The article examines such a phenomenon as cybercrime, indicates and analyzes its scale, and also suggests measures that can be used to combat it. The question of the use of biometric systems in information systems from the point of view of ensuring information security is raised. The risks that may arise as a result of the use of biometric systems are highlighted, and recommendations for preventing such risks are outlined.

Keywords: cybercrime, information society, biometric system, biometric data, personal data, information technology, cybercriminals, Internet.

Кузбагаров Артур Муслимович

Студент,

Санкт-Петербургский государственный архитектурно-строительный университет
(г. Санкт-Петербург, Российская Федерация)

artur.kuzbagarov.00@mail.ru

Научный руководитель – Е. В. Кузбагарова, кандидат юридических наук, доцент,
доцент кафедры судебных экспертиз**ВІМ-МОДЕЛИРОВАНИЕ В ПРОИЗВОДСТВЕ СУДЕБНОЙ
СТРОИТЕЛЬНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ**

Аннотация: В статье рассматриваются вопросы применения ВІМ-моделирования в процессе производства судебной строительно-технической экспертизы, с указанием возможностей внедрения новой технологии в экспертную деятельность, а также целей и задач, которые решаются при помощи использования созданной ВІМ-модели в рамках производства судебной экспертизы.

Ключевые слова: ВІМ-моделирование, информационная модель, строительный объект, судебный эксперт, судебная строительно-техническая экспертиза.

Для цитирования:

Кузбагаров А. М. ВІМ-моделирование в производстве судебной строительно-технической экспертизы // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 478–483.

В настоящее время не является проблемой получение информации о ВІМ-моделировании, в частности Информационный ресурс о ВІМ-моделировании¹ и иные сайты позволяют получить массу информации в данном направлении. Однако в данной статье наше внимание будет обращено на использование ВІМ-моделирования в деятельности инженеров-строителей и, в частности, в рамках деятельности инженера-

строителя, выступающего в качестве судебного эксперта и применяющего ВІМ-моделирование при производстве судебной строительно-технической экспертизы.

В сфере строительства, в соответствии с Планом мероприятий («дорожная карта») поэтапного внедрения технологий информационного моделирования в области промышленного и

¹ Информационный ресурс о ВІМ-моделировании. URL: <https://1-bim.ru/нормативная-документация-по-bim>; Проектно-инжиниринговая компания.

Лаборатория ВІМ-технологий – Bimlab. URL: <https://bimlab.ru/faq-bim3d.html> (дата обращения 12.02.2021).

гражданского строительства², активно осуществляется переход на обязательное использование технологий информационного моделирования при выполнении инженерных изысканий, проектировании, строительстве и эксплуатации капитальных объектов различного назначения. Данный переход осуществляется поэтапно согласно Приказа Министерства строительства и жилищно-коммунального хозяйства РФ от 29 декабря 2014 г. № 926/пр «Об утверждении Плана поэтапного внедрения технологий информационного моделирования в области промышленного и гражданского строительства»³. Применение BIM-технологий можно считать новым этапом в развитии строительства и эксплуатации зданий. BIM-технологии позволяют создавать не только 3D-модели зданий и сооружений, но и осуществлять полный расчёт жизненного цикла сооружения, с учетом содержащейся информацией о материалах, используемых при строительстве и эксплуатации зданий, сроках текущего и капитального ремонта, использовании инженерных сетей в режиме виртуальной

реальности. Вместе с тем активное внедрение BIM-технологий потребовало создания единого стандарта применения BIM-технологий в области промышленного и гражданского строительства. В качестве стандарта на данном этапе законодательного закрепления создания BIM-модели (информационной модели) можно рассматривать:

- п. 10.3 ст. 1, ст. 57.5 Градостроительного кодекса Российской Федерации⁴ «Информационная модель объекта капитального строительства»;
- правила формирования и ведения информационной модели, определенные Постановлением Правительства РФ от 15.09.2020 № 1431 «Об утверждении Правил формирования и ведения информационной модели объекта капитального строительства, состава сведений, документов и материалов, включаемых в информационную модель объекта капитального строительства и представляемых в форме электронных документов, и требований к форматам указанных электронных документов, а также о внесении изменения в пункт 6 Положения о выполнении инженерных

² План мероприятий («дорожная карта») поэтапного внедрения технологий информационного моделирования в области промышленного и гражданского строительства // СПС «КонсультантПлюс» URL: http://www.consultant.ru/document/Cons_doc_LAW_362458/#dst100013 (дата обращения 17.02.2021).

³ Приказ Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 29 декабря 2014 года № 926/пр «Об утверждении Плана поэтапного внедрения технологий

информационного моделирования в области промышленного и гражданского строительства» // Официальный сайт министерства строительства и жилищно-коммунального хозяйства РФ. URL: <http://www.minstroyrf.ru/docs/2663/> (дата обращения: 17.02.2021).

⁴ Градостроительный кодекс Российской Федерации от 29.12.2004 № 190-ФЗ (ред. от 02.08.2019) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_51040/ (дата обращения 17.02.2021).

изысканий для подготовки проектной документации, строительства, реконструкции объектов капитального строительства»⁵;

– ГОСТ, например – ГОСТ Р 57311-2016 «Моделирование информационное в строительстве. Требования к эксплуатационной документации объектов завершеного строительства» и другие;

– Свод правил, в частности СП 328.1325800.2017 «Информационное моделирование в строительстве. Правила описания компонентов информационной модели»; СП 331.1325800.2017 «Информационное моделирование в строительстве. Правила обмена между информационными моделями объектов и моделями, используемыми в программных комплексах»; СП 333.1325800.2017 «Информационное моделирование в строительстве. Правила формирования информационной модели объектов на различных стадиях жизненного цикла»; СП 404.1325800.2018 «Информационное моделирование в строительстве. Правила разработки планов проектов, реализуемых с применением технологии информационного моделирования» и другие.

При создании BIM-модели инженеру-строителю необходимо руководствоваться всеми

вышеуказанными нормативными актами, при этом судебный эксперт инженер-строитель не является исключением. Вместе с тем цели использования BIM-модели различны в рамках строительства и в процессе производства судебной строительно-технической экспертизы. Судебная строительно-техническая экспертиза (далее ССТЭ) имеет важное значение при расследовании и судебном разбирательстве уголовных дел о причинах разрушений и несчастных случаев в строительстве, при рассмотрении споров в судах общей юрисдикции и арбитражных судах о стоимости и качестве зданий, строений и сооружений, при установлении правильности и правомерности строительства при расследовании дел об административных правонарушениях. В строительстве моделирование применяется в тех случаях, когда экспериментировать со строительным объектом используя физические приемы невозможно или нецелесообразно. Например, когда объект находится в разрушенном состоянии и надо определить причину разрушения или если он находится в предаварийном состоянии и может разрушиться в любой момент времени. В первом случае применение данного метода позволит восстановить картину происшествия, во втором случае исследование объекта становится

⁵ Постановление Правительства РФ от 15.09.2020 № 1431 «Об утверждении Правил формирования и ведения информационной модели объекта капитального строительства, состава сведений, документов и материалов, включаемых в информационную модель объекта капитального строительства и представляемых в форме электронных документов, и требований к форматам

указанных электронных документов, а также о внесении изменения в пункт 6 Положения о выполнении инженерных изысканий для подготовки проектной документации, строительства, реконструкции объектов капитального строительства» // СПС «Гарант» URL: <https://www.garant.ru/products/ipo/prime/doc/74544278/> (дата обращения 18.02.2021).

небезопасным. В этих случаях у судебного эксперта строителя появляется возможность использовать модели объектов для получения доказательственной базы при производстве экспертизы. В процессе экспертного исследования эксперт может не только самостоятельно разрабатывать модель, но и работать с уже имеющимися в его распоряжении графическими моделями и BIM-моделями.

Созданная BIM-модель позволяет использовать информацию со всех этапов строительства, о материалах и оборудовании, которое используется в процессе, информацию о бригадах и руководителях и так далее. За счет непрерывного обновления информации создается база данных, которая используется, чтобы предвидеть и исключить возможные проблемы при строительстве⁶. Тот факт, что созданная модель существует не только в процессе строительства, но продолжается храниться и после его окончания играет важную роль в осуществлении ССТЭ. Вместо предоставления эксперту документации о здании или сооружении в бумажном виде в нескольких томах, полностью на электронном носителе будет представлена модель, содержащая полную и актуальную информацию с возможностью узнать состоянии в

предыдущие периоды времени. Помимо того, как создана модель объекта, у эксперта появляется возможность проводить вычислительный эксперимент, который заключается в прогнозировании будущего состояния. Данная возможность является перспективой для судебного эксперта в доказывании и проверке собственных гипотез. Для того чтобы пользоваться BIM-моделями эксперт должен обладать специальными знаниями, иначе он не сможет оказать помощь суду, органам дознания, назначившим экспертизу. Следует помимо развития и продвижения идей моделирования в стране создать возможность экспертам проходить обучение, дабы соответствовать повышенным требованиям к их специальным познаниям⁷.

Таким образом моделирование незаменимый спутник эксперта-строителя на протяжении его карьеры, и разработка методов моделирования важна для своевременного, качественного выполнения им своей работы. Эксперты часто сталкиваются с задачами, которые под силу решить только с помощью кибернетических методов с применением моделирования, в частности математического. Возможности данных моделей с каждым годом становятся все

⁶ Харченко В. Б., Иванов Д. В. Актуальные вопросы судебных строительно-технических экспертиз // Вопросы экспертной практики. 2019. № 51. С. 672. URL: <https://www.elibrary.ru/item.asp?id=39657968> (дата обращения 12.02.2021). Режим доступа: Научная электронная библиотека eLIBRARY.RU (для зарегистрированных пользователей).

⁷ Харченко В. Б. Использование BIM-моделей при производстве судебной строительно-технической экспертизы // Юридическая наука. 2019. № 11. С. 90. URL: <https://cyberleninka.ru/article/n/ispolzovaniya-bim-modeley-pri-proizvodstve-sudebnoy-stroitelno-tehnicheskoy-ekspertizy> (дата обращения 12.02.2021). Режим доступа: Научная электронная библиотека «КиберЛенинка».

обширнее за счет использования более современных вычислительных средств, которые позволяют проводить больше расчетов за короткое время. Использование метода моделирования в ССТЭ в настоящее время наиболее эффективно в рамках умения работы с программами AutoCAD, Autodesk Revit, ArchiCAD, ЛИРА–САПР, САПФИР и т. п. Основная направленность программы AutoCAD – 3D–моделирование. Благодаря широчайшему набору инструментов и настроек, эксперт может создать любой сложности объект. Использование программы Autodesk Revit, ArchiCAD позволяет эксперту осуществлять параметрическое моделирование в процессе производства судебной строительно-технической экспертизы. В частности, например, судебному эксперту целесообразно создать BIM-модель здания с использованием программного обеспечения на платформе ArchiCAD и провести комплекс исследовательских работ с последующим импортированием модели в формате IFC в ПК ЛИРА–САПР. Рабочая документация эксперта с рекомендациями по устранению имеющихся разрушений, нарушений целостности основания, фундамента, конструкций и элементов здания (сооружения), может быть создана в ПК NAnoCAD.

Применение данных программ позволит эксперту при внесении данных, полученных в процессе осмотра и соответствующих измерений, в базу данных программ, создать модель с имеющимися данными и увидеть их некорректность к данному строительному объекту и многие иные моменты, допущенные в процессе строительства и позволяющие эксперту сделать вывод и дать ответ на поставленный перед экспертом вопрос.

На основании вышеизложенного можно сделать вывод, что BIM-технологии несмотря всю свою привлекательность для сферы строительства, пока не активно используется в процессе всего жизненного цикла строительного объекта. В качестве главных препятствий активной реализации «дорожной карты» можно выделить недостаточная нормативно-правовая база, регулирующая стадии жизненного цикла строительного объекта капитального строительства, а также непосредственно процесс внедрения и использования BIM-технологий и созданных на их применении информационных моделей. Как следствие, наличие данных вопросов проекционным образом находит отражение и в иных сферах применения BIM-технологий и, в частности, в судебно-экспертной деятельности.

Список литературы

1. Харченко В. Б. Актуальные вопросы судебных строительно-технических экспертиз / В. Б. Харченко, Д. В. Иванов // Вопросы экспертной практики. 2019. № S1. С. 669–676. URL: <https://www.elibrary.ru/item.asp?id=39657968> (дата обращения 12.02.2021). Режим доступа: Научная электронная библиотека eLIBRARY.RU (для зарегистрир. пользователей).

2. Харченко В. Б. Использование BIM-моделей при производстве судебной строительно-технической экспертизы // Юридическая наука. 2019. № 11. С. 89–91. URL: <https://cyberleninka.ru/article/n/ispolzovaniya-bim-modeley-pri-proizvodstve-sudebnoy-stroitelno-tehnicheskoy-ekspertizy> (дата обращения 12.02.2021). Режим доступа: Научная электронная библиотека «КиберЛенинка».

Artur M. Kuzbagarov

Student,

Saint Petersburg State University of Architecture and Civil Engineering

(Saint Petersburg, Russian Federation)

artur.kuzbagarov.00@mail.ru

Scientific supervisor – E. V. Kuzbagarova, PhD (Law), Associate Professor, Associate Professor of the Department of Forensic Expertise

BIM-MODELING IN PRODUCTION OF FORENSIC CONSTRUCTION-TECHNICAL EXPERTISE

Abstract: The article discusses the application of BIM-modeling in the production of forensic construction and technical expertise, indicating the possibilities of introducing new technology into expert activities, as well as the goals and objectives that are solved using the created BIM-model in the framework of the forensic examination.

Keywords: BIM modeling, information model, construction object, forensic expert, forensic construction and technical expertise.

УДК: 34.06

Курбанова Фарахноз Хурshedовна

Студент,

МИРЭА – Российский технологический университет
(РТУ МИРЭА)

(г. Москва, Российская Федерация)

khurshed.kurbanov@mail.ru

Научный руководитель – А. П. Забайкалов, кандидат юридических наук, доцент

**ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ**

Аннотация: В статье рассматриваются различные современные технологии, которые на данный момент применяются в правоохранительной сфере, а также исследуются технологии, которые могли бы повысить эффективность деятельности правоохранительных органов. Приводятся примеры результатов работы некоторых технологий на данный момент.

Ключевые слова: технологии, правоохранительные органы, искусственный интеллект, автоматизированные системы, искусственный интеллект.

Для цитирования:

Курбанова Ф. Х. Использование современных компьютерных технологий в правоохранительной деятельности // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 484–488.

В современном мире компьютеризация деятельности играет колоссальную роль. На данном этапе практически во всех сферах происходит активное внедрение информационных технологий в рабочий процесс. Данная тенденция не обошла и правоохранительную деятельность. В ней существует множество аспектов, которым необходима компьютеризация. Это поможет ускорить работу, повысить ее точность и, соответственно, качество.

Система правоохранительных органов является важным звеном всего государства. Поэтому перед Россией

стоит цель тотальной компьютеризации данной системы. В ее задачи входят повышение объективности деятельности, ее прозрачности, обеспечение оперативного электронного взаимодействия между государственными органами, гражданами и различными организациями.

Информационные технологии обладают множеством плюсов. На нынешнем этапе развития они не просто исполняют конкретный алгоритм действий, который задал им человек, они самостоятельно

регулируют данные алгоритмы, опираясь на существующий опыт. Помимо этого, компьютер способен обработать куда больший поток информации в короткий срок, а также ему не требуется отдых и сон.

Современные технологии строятся на нескольких основополагающих принципах. К ним относятся удобство редактирования уже заданных данных, изменение поставленных задач; дружелюбный и интуитивно понятный интерфейс; возможность легкой интеграции работы в иные программы. Также выделяют множество видов сами технологий по цели их работы. Например, некоторые из них направлены на обработку данных, автоматизацию жизнедеятельности офисов, поддержку принятия решений.

Можно выделить целый ряд различных автоматизированных информационных систем, которые выполняются совершенно разнообразные задачи. К ним относятся автоматизированные: информационно-поисковые системы, системы обработки данных, информационно-справочные системы, системы управления, а также экспертные системы. Данные технологии могут совершенно различным образом комбинироваться и объединяться¹.

Эти системы выполняют множество задач и невероятно облегчают, и ускоряют работу правоохранительных органов. Они служат для поиска, выдачи и отбора правовой информации по запросам; выдают справки по различной

оперативной информации; обеспечивают руководство служебной информацией. Также к важным технологиям, которые применяются в правоохранительных органах на данном этапе, относится система автоматизированного рабочего места. Данная система представляет собой ряд программных и технических средств автоматизации рабочего процесса. Обычно к ним относятся персональные компьютеры, сканеры, принтеры, средства сетевой связи, офисные приложения, электронные таблицы, графические и текстовые процессоры.

Как указывалось выше, на данный момент в органах ОВД активно применяется множество автоматизированных информационно-справочных систем (далее АИСС). Говоря о конкретных примерах, можно привести следующее, система «Гастролеры» содержит данные о вещах и лицах, которые были похищены на транспорте и имели характерные индивидуальные признаки. АИСС «Сводка» предоставляет оперативную информацию о преступлениях и событиях. Автоматизированные информационно-поисковые системы «Красители», «Оружие», «Наркотические средства» и др. направлены на судебно-экспертную и криминалистическую деятельность. Также существует Федеральный банк криминальной информации. Автоматизированный программный комплекс «Безопасный город» предусматривает масштабное использование системы видео

¹ Бурыченко В. В., Пахирка А. И. Методы слежения за объектами с применением

глубокого обучения // Сибирский журнал науки и технологий. 2020. № 2. С. 152.

мониторинга в пределах городских поселений².

Тем не менее, несмотря на эффективность перечисляемых выше систем, существуют иные технологии, которые смогут поднять деятельность правоохранительных органов на несколько ступеней вверх. Речь идет о таких современных технологиях и методах, как Big data, Legal tech, Deep Learning.

Сфера правоохранительной деятельности нуждается в высоком уровне безопасности. Для обеспечения подобного отлично подойдет технология Big data. Ее суть заключается в возможности обработки колоссальных массивов данных, также в условиях их постоянного роста. Отмечается, что данная технология является одной из самых быстрорастущих, объемы, которые она способна обрабатывать, удваиваются каждые полтора года³. Сфер применения у Big data немыслимое множество. Ее можно применять для предупреждения преступлений в сети Интернет, пресечения незаконного оборота запрещенных предметов, организации безопасного дорожного движения, быстрый поиск вирусного ПО. Данная технология позволит сильно повысить оперативность работы правоохранительных органов, позволит прогнозировать эффективность различных решений, а также сыграет роль дополнительной защиты.

Для правоохранительной деятельности крайне актуальной является технология «Legal tech». Она создана для информационного обслуживания юристов и имеет широкое распространение в США. Данные технологии позволяют оперативно анализировать судебные решения, проводить оценку перспективности того или иного судебного дела, выделять ключевые аспекты и правовые вопросы спора для судей, а также подготавливать необходимые юридические документы в автоматическом режиме.

Важной частью деятельности Legal tech является их направленность на проведение примирительных процедур. Одной из функций данных технологий является разработка инструментов, которые позволят оценить обстоятельства дела обычным гражданам, не являющимся юристами. Все указанные выше функции значительно скажутся на стоимости юридических услуг, они станут в разы доступнее для населения⁴.

Крайне благоприятное влияние на деятельность правоохранительной системы оказала бы технология Deep Learning. В настоящее время данная технология является наиболее эффективной для создания глубинных нейронных сетей и искусственного интеллекта. Они способны автоматически выделить из данных наиболее необходимые признаки, которые нужны для решения той или

² Авдеева Е. В., Гордей В. А. Оптимизация деятельности правоохранительных органов в контексте внедрения информационно-коммуникационных технологий // Закон и право. 2018. № 10. С. 94.

³ Абдыкаримова А. Т. Big Data: проблемы и технологии // Международный журнал

гуманитарных и естественных наук. 2019. № 5. С. 18.

⁴ Гвоздецкий Д. С. Legal Tech и ведомственное нормотворчество: перспективы // Образование. Наука. Научные кадры. 2020. № 4. С. 34.

иной задачи. Данные функции активно применяются для создания систем распознавания лиц и речи, поиска схожих объектов, вычисления вредоносных программ и так далее⁵.

В данный момент правительство Российской Федерации уже ведет активную работу над продолжением автоматизации юридической и правоохранительной деятельности. В 2017 году была принята программа «Цифровая экономика», в положения которой заложена концепция автоматизации нормотворчества, использование множества технологий, построенных на искусственном интеллекте, технологии виртуальной реальности и многое другое. Использовать все это можно в абсолютно разных аспектах правоохранительной деятельности. Моделирование эпизодов преступлений при помощи виртуальной реальности, розыск лиц путем мониторинга систем видео фиксации, оптимизация дорожного движения, реализуемая при помощи система считывания помех на дороге и дорожных знаков. Все это очень сильно повысит эффективность работы правоохранительных органов⁶.

Система распознавания лиц уже работает в тестовом режиме. Так, по данным статьи за 2019 год: «В московском метро система VisionLabs помогла задержать около сотни человек, из которых 62 находились в федеральном розыске, остальные проходили по другим контрольным базам». И, исходя из информации, предоставленной в ней же: «По данным департамента информационных технологий, благодаря наружной городской системе видеоаналитики с августа 2017 г. задержано 39 человек – ДИТ регулярно проводит разные тесты. В том числе ДИТ тестировал систему на 17 массовых мероприятиях этого и прошлого года – там полиция задержала 152 человека»⁷.

Таким образом, применение инновационных технологий позволит значительно повысить эффективность правоохранительных органов, уровень прозрачности их деятельности, оперативность реализации задач правосудия и правопорядка. Также данные технологии помогут снизить риски коррупции и повысить доступность юридических услуг для населения.

Список литературы

1. Абдыкаримова А. Т. Big Data: проблемы и технологии // Международный журнал гуманитарных и естественных наук. 2019. № 5. С. 17–20.

⁵ Бурыченко В. В., Пахирка А. И. Методы слежения за объектами с применением глубокого обучения // Сибирский журнал науки и технологий. 2020. № 2. С. 152.

⁶ Никитин Е. В. О новых возможностях применения современных цифровых технологий в правоохранительной

деятельности // Правопорядок: история, теория, практика. 2018. № 4. С. 57.

⁷ Миллер Л. МВД подвело итоги тестовой работы систем распознавания лиц в Москве // «Ведомости» Дата обновления: 27.06.19. URL: <https://www.vedomosti.ru/technology/articles/2019/06/26/805163-mvd-podvelo> (дата обращения: 24.04.2021).

2. Авдеева Е. В. Оптимизация деятельности правоохранительных органов в контексте внедрения информационно-коммуникационных технологий / Е. В. Авдеева, В. А. Гордей // Закон и право. 2018. № 10. С. 93–95.
3. Бурыченко В. В. Методы слежения за объектами с применением глубокого обучения / В. В. Бурыченко, А. И. Пахирка // Сибирский журнал науки и технологий. 2020. № 2. С. 150–154.
4. Гвоздецкий Д. С. Legal Tech и ведомственное нормотворчество: перспективы // Образование. Наука. Научные кадры. 2020. № 4. С. 33–35.
5. Миллер Л. МВД подвело итоги тестовой работы систем распознавания лиц в Москве // «Ведомости». Дата обновления: 27.06.19. <https://www.vedomosti.ru/technology/articles/2019/06/26/805163-mvd-podvelo>.
6. Никитин Е. В. О новых возможностях применения современных цифровых технологий в правоохранительной деятельности // Правопорядок: история, теория, практика. 2018. № 4. С. 55–59.

Farakhnoz K. Kurbanova

Student,

MIREA – Russian Technological University

(RTU MIREA)

(Moscow, Russian Federation)

khurshed.kurbanov@mail.ru

Scientific supervisor – A. P. Zabaykalov, PhD (Law), Associate Professor

THE USE OF MODERN COMPUTER TECHNOLOGIES IN LAW ENFORCEMENT

Abstract: The article examines various modern technologies that are currently used in the law enforcement sphere, and examines technologies that could increase the efficiency of law enforcement agencies. Examples of the results of the work of some technologies now are given.

Keywords: technologies, law enforcement agencies, artificial intelligence, automated systems, artificial intelligence.

УДК 343.98

Кускова Виктория Анатольевна

Студент,

Национальный исследовательский Нижегородский государственный университет
имени им. Н. И. Лобачевского
(г. Нижний Новгород, Российская Федерация)
vickus25@mail.ru

Цибирева Анна Сергеевна

Студент,

Национальный исследовательский Нижегородский государственный университет
имени им. Н. И. Лобачевского
(г. Нижний Новгород, Российская Федерация)
anna.tsibireva.99@mail.ru

Научный руководитель – А. В. Полякова, старший преподаватель кафедры
судебной экспертизы юридического факультета

ПРИМЕНЕНИЕ МЕТОДА ТРЕХМЕРНОГО МОДЕЛИРОВАНИЯ В ЦЕЛЯХ УСТАНОВЛЕНИЯ ХРОНОЛОГИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ВЫПОЛНЕНИЯ ПЕРЕСЕКАЮЩИХСЯ ШТРИХОВ

Аннотация: В статье рассматривается возможность применения метода трехмерного моделирования в целях установления относительной давности реквизитов документа. В основу данной научной работы положены результаты проведенного научно-практического исследования, в рамках которого были созданы 3D-модели пересекающихся штрихов и исследованы.

Ключевые слова: установление относительной давности реквизитов документа, пересекающиеся штрихи, 3D-модели, метод трехмерного моделирования, технико-криминалистическая экспертиза документов.

Для цитирования:

Кускова В. А. Применение метода трехмерного моделирования в целях установления хронологической последовательности выполнения пересекающихся штрихов / В. А. Кускова, А. С. Цибирева // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 489–496.

Актуальной задачей технико-криминалистической экспертизы документов по-прежнему является установление хронологической последовательности выполнения пересекающихся реквизитов

документов, которая в свою очередь позволяет выявить факт изменения первоначального содержания текста в документе путем дописки (допечатки, дорисовки), а также выявить относительную последовательность

нанесения отдельных реквизитов в документе, как правило подписей, оттисков печатей и штампов, числовых обозначений, и относится к числу наиболее трудных задач, что обусловлено целым рядом объективных факторов, описываемых в учебной и научной литературе¹.

На наш взгляд, можно выделить два взаимосвязанных между собой фактора, относящих данную задачу к трудноразрешимым. Во-первых, это объясняется спецификой самого объекта – пересекающимися штрихами, которые выполняются и наносятся материалами письма, различными по своей природе, в силу чего их распределение по слою бумаги зависит от степени вязкости самого красящего вещества и плотности бумаги, так, например, глубоко в толщу бумаги проникают красящие вещества штемпельной краски, капиллярной и перьевой ручки, что в свою очередь в большинстве случаев дает «ложную картину», которая образуется на участке пересечения их с другими красящими веществами материалов письма. И, во-вторых, закономерно вытекает следующий фактор – отсутствие методики исследования пересекающихся штрихов, которая бы давала точную и однозначную картину.

На сегодняшний день экспертная практика оперирует большим перечнем методов² в целях установления последовательности

выполнения пересекающихся штрихов реквизитов документов, в числе которых микроскопические методы; адсорбционно-люминесцентный метод; сканирующая электронная микроскопия; профилирование; механическое удаление верхнего слоя на участке пересечения; изучение ИК-спектров нарушенного полного внутреннего отражения (FTIR) на участках пересечения, исследование следов давления штрихов на аппарате электростатического обнаружения (ESDA) и др.³ С одной стороны, указанный перечень обусловлен тем, что зачастую один метод не может дать надежных результатов, что требует применения комплекса методов, с другой – каждый из методов имеет свои ограничения, обусловленные как возможностями самого метода, так и особенностями материалов письма в исследуемых пересекающихся штрихах. Стоит отметить, что эксперту приходится в каждом конкретном случае вновь апробировать применяемые методы на экспериментальных пересечениях, выполняемых материалами письма – аналогами, в двух заведомых вариантах их взаимного расположения, без учета этого условия полученные результаты могут дать искаженную картину реального взаимного расположения реквизитов в исследуемом документе.

разрушающими и вносящими изменения в первоначальное содержание документа.

³ Торопова М. В. Криминалистическая экспертиза установления относительной давности выполнения реквизитов документов: дис. ... канд. юрид. наук. Москва, 2014. 202 с.

¹ Скрипченко А. В., Коровкин Д. С. Техникo-криминалистическая экспертиза документов: учебник. СПб.: Санкт-Петербург. ун-т МВД России, 2014. Ч. II. 212 с.

² Большинство методов, которые могут дать положительный результат, являются

Все это создает трудности в работе эксперта, не дает возможности оптимизировать ее и в большинстве случаев эксперты вынуждены формулировать вывод в форме «не представляется возможным» (нпв).

Перспективным направлением в судебно-экспертной практике является применение метода трехмерного моделирования объектов (явлений) в целях установления обстоятельств, имеющих значение для дела посредством их исследования. Применение методов трехмерного моделирования относится к практике зарубежных правоохранительных органов, которые отмечают эффективность использования методов 3D-сканирования и 3D-моделирования при работе со следами по сравнению с традиционными методами, которые могут вносить изменения в объекты, вплоть до полного их разрушения, что, несомненно, сказывается на качестве расследования. Большее развитие указанный метод получил в судебно-медицинской практике, в частности, для фиксации и последующего анализа повреждений на костях и мягких тканях⁴; установления пола жертвы на основании компьютерного изучения трехмерного изображения черепа⁵ и др. Однако на сегодняшний

момент указанный метод активно начал применяться и в криминалистическом направлении, а именно при работе со следами преступления на месте происшествия и дальнейшем исследовании экспертами трехмерных изображений изъятых следов и использовании их при доказывании следователями.

Существует два способа получения трехмерной копии объекта: трехмерное сканирование и создание модели на базе цифровых изображений.

О возможности применения методов трехмерного моделирования в целях установления последовательности пересекающихся штрихов реквизитов документа указывали в Институте судебной экспертизы Московского университета МВД России имени В. Я. Кикотя⁶. Были наглядно показаны возможности 3D-микроскопа Leica DVM6, сочетающего в себе функции оптического микроскопа и лазерного профилометра, который предназначен для точных и достоверных измерений, а также для построения пространственных изображений. Полученное с такого микроскопа трехмерное изображение места пересечения штрихов позволяет благодаря просматриваемому

⁴ Feasibility of contactless 3D optical measurement for the analysis of bone and soft tissue lesions: new technologies and perspectives in forensic sciences / G. Sansoni, C. Cattaneo, M. Trebeschi [et al.] // Journal of forensic sciences. 2009. Vol. 54, № 3. P. 540–545.

⁵ Improving sex estimation from crania using a novel three-dimensional quantitative method [Определение половой принадлежности по черепу с использованием нового метода

трехмерного анализа] / E. E. Abdel Fatah, N. R. Shirley, R. L. Jantz [et al.] // Journal of forensic sciences. 2014. Vol. 59, № 3. P. 590–600.

⁶ Горбулинская И. Н., Барбачакова Ю. Ю., Шавленко Е. В. О возможностях применения методов 3D-моделирования в ходе производства криминалистических экспертиз // Вестник экономической безопасности. 2018. № 1. С. 42–45.

рельефу штриха, а также наслоению красящего вещества определить даже штрихи, выполненные однородными материалами письма, например, пастой шариковых ручек.

Метод трехмерного моделирования имеет явные преимущества перед традиционными методами исследования пересекающихся штрихов, однако указанный микроскоп является дорогостоящим и вряд ли в будущем возможно оснастить каждое экспертное подразделение таким оборудованием. Сегодня подобными микроскопами располагают лишь единичные негосударственные экспертные учреждения.

На основе имеющихся знаний о методе трехмерного моделирования было проведено научно-практическое исследование с целью проверки возможности моделирования пересекающихся штрихов в программе Agisoft Metashape 1.7.2. Для этой цели были взяты материалы письма, оставляющие следы нажима в штрихах: шариковые ручки и перьевая ручка, а также тонер, нанесенный на лист бумаги наиболее плотным слоем, что придало ему рельефность.

На первом этапе в целях достоверности методики были выполнены шесть экспериментальных пересечений: двумя шариковыми ручками; шариковой ручкой и перьевой ручкой; тонером и шариковой ручкой, – в двух заведомых вариантах их взаимного расположения.

На втором этапе на МСКК-5 с кратностью увеличения 5^x с помощью закрепленного на нем цифрового фотоаппарата Canon EOS 550 D были получены 360-градусные панорамы (фотографии штрихов под различными углами) указанных штрихов, необходимые для построения будущих моделей в программном обеспечении Agisoft Metashape.

На третьем этапе на основе цифровых фотографий штрихов программа Agisoft Metashape версия 1.7.2. осуществила автоматизированное создание трехмерных моделей штрихов. Построение модели начинается с того, что после загрузки исходных фотографий Metashape осуществляет поиск общих точек для определения положения и ориентации камеры для каждого кадра. Результатом операции является разреженное облако точек в трехмерном пространстве модели, необходимое для визуальной оценки качества выравнивания фотографий. Далее Metashape, используя данные о расположении камер, выполняет построение плотного облака точек, на основе которого строит трехмерную поверхность (полигональную модель) и текстуру объекта. Как результат, были получены детальные и точные модели пересекающихся штрихов⁷.

На четвертом этапе штрихи были исследованы, в ходе чего установлено что:

- Штрих № 1 расположен под штрихом № 2 на основании видимого рельефа и смещения штриха № 1

⁷ Руководство пользователя Agisoft Metashape Professional Edition, версия 1.5 // Agisoft: официальный сайт. Дата

публикации: 2019. URL: https://www.agisoft.com/pdf/metashape-pro_1_5_ru.pdf (дата обращения: 13.05.2021).

относительно общей линии направления движения штриха в месте пересечения со штрихом № 2 (Рис. 1).

- Штрих № 2 расположен под штрихом № 1 на основании видимого рельефа, отсутствия смещения штриха № 1 относительно общей линии направления движения штриха в месте пересечения со штрихом № 2 (Рис. 2).

- На левом изображении штрих, выполненный чернилами перьевой ручки (1), расположен под штрихом, выполненным пастой шариковой ручки (2), на правом изображении штрихи, выполненные аналогичными материалами письма, расположены наоборот (штрих № 1 расположен поверх штриха № 2) на основании сравнения различия в рельефности штрихов, в первом случае рельеф от шариковой ручки хорошо заметен и вдавливают штрихи перьевой ручки, в другом случае, так как штрих пасты шариковой ручки

лежат снизу, различия в рельефе штрихов практически нет (Рис. 3).

- На левом изображении штрих, нанесенный тонером (1), расположен поверх штриха, выполненного пастой шариковой ручки (2), на правом изображении штрихи, выполненные аналогичными материалами письма, расположены наоборот (штрих № 1 расположен под штрихом № 2) на основании сравнения различия в рельефности штрихов и интенсивности красящего вещества в штрихах, в первом случае из-за толстого слоя пасты шариковой ручки частицы тонера в месте пересечения имеют неокрашенные участки, при этом рельеф практически отсутствует, в другом случае образуется рельеф и вдавленность тонера пастой шариковой ручки, также имеется радужный перелив, образованный скоплением частиц пасты шариковой ручки.

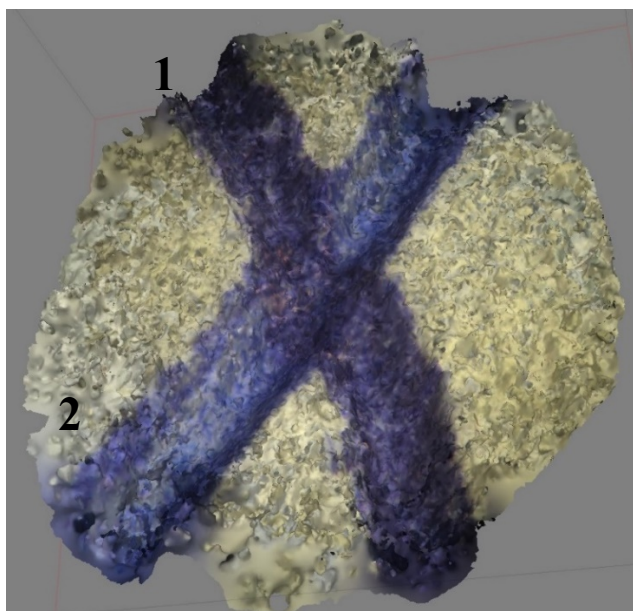


Рис. 1. 3D-модель места пересечения штрихов, выполненных однородным красящим веществом – пастой шариковых ручек.



Рис. 2. 3D-модель места пересечения штрихов, выполненных однородным красящим веществом – пастой шариковых ручек (обратная картина).

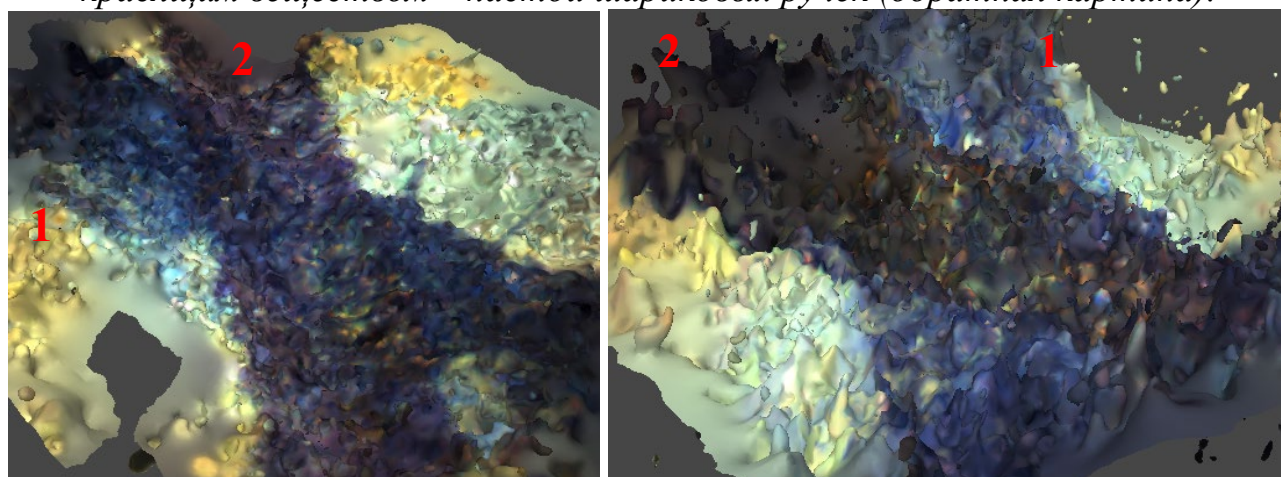


Рис. 3. 3D-модели места пересечения штрихов, выполненных различными красящими веществами – чернила перьевой ручки и паста шариковой ручки (в двух различных вариантах).

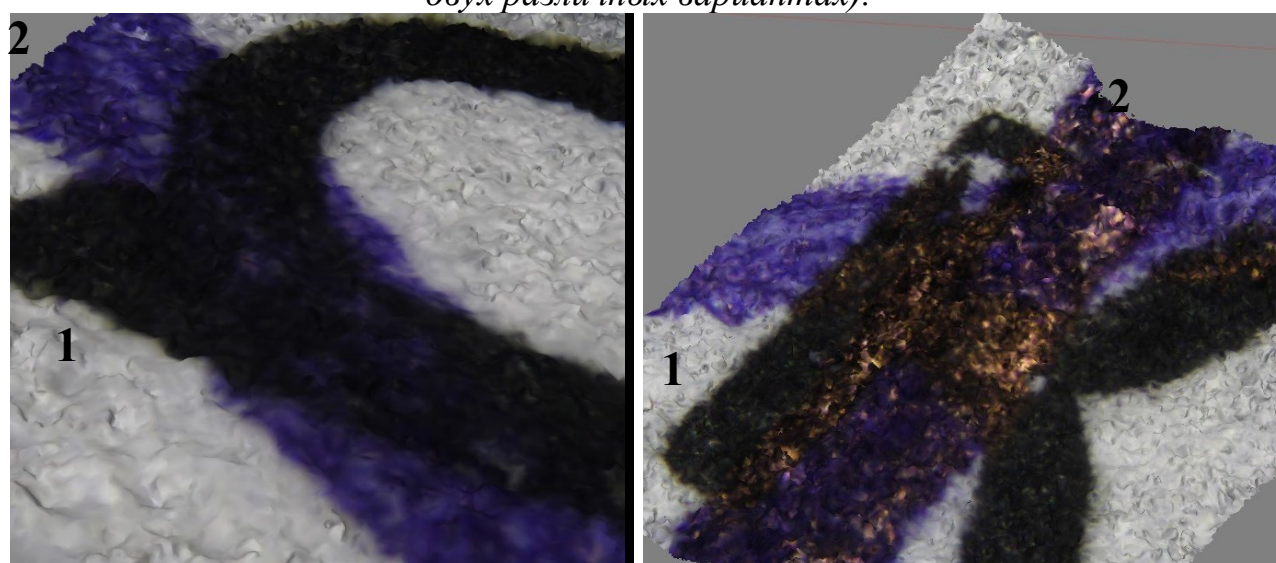


Рис. 4. 3D-модели места пересечения штрихов, выполненных различными красящими веществами – электрофотографический тонер и паста шариковой ручки (в двух различных вариантах).

На основании исследования 3D-моделей пересекающихся штрихов, следует отметить, что метод следует эффективно применять, когда на участках пересечения имеются явные следы давления, а сами штрихи достаточно интенсивные.

Таким образом, методика установления относительной давности выполнения в документах двух рукописных записей (подписей), выполнения электрофотографического печатного текста и рукописных записей (подписей) в документах методом трехмерного моделирования имеет целый ряд преимуществ:

- является не разрушающим, бесконтактным и дающим однозначную картину (положительный результат);
- оптимизирует работу эксперта (не требуется использовать комплекс методов);
- экономична (используется обычный микроскоп с кратностью

увеличения от 5^x и более, фотоаппарат и установленное на компьютере ПО фотограмметрии, что доступно практически в каждом экспертном учреждении);

- работает с пересекающимися штрихами выполненными как однородными, так и различными материалами письма.

На основании вышеизложенного можно сделать вывод, что для повышения эффективности работы экспертов в области ТКЭД следует обратить внимание на проверенный в ходе проведенного исследования метод и использовать его в экспертной деятельности для определения пересекающихся штрихов, однако стоит отметить, что специфика метода открывает его возможности при исследовании и других материалов письма, которые не были рассмотрены в данной работе, что требует дальнейшего изучения.

Список литературы

1. Аверьянова Т. В. Судебная экспертиза. Курс общей теории. М.: Норма, 2009. 480 с.
2. Горбулинская И. Н. О возможностях применения методов 3D-моделирования в ходе производства криминалистических экспертиз / И. Н. Горбулинская, Ю. Ю. Барбачакова, Е. В. Шавленко // Вестник экономической безопасности. 2018. № 1. С. 42–45.
3. Полякова А. В. К вопросу о перспективах применения 3D-технологий в судебно-экспертной деятельности // Международные и национальные тенденции и перспективы развития судебной экспертизы: сборник докладов II Международной научной конференции (г. Нижний Новгород, 21–22 мая 2020). Н. Новгород: ННГУ, 2020. С. 226–232.
4. Полякова А. В. Перспективы использования 3D-моделирования и 3D-печати при производстве некоторых криминалистических экспертиз // Материалы VI Международной научно-практической конференции «Уголовное производство: процессуальная теория и криминалистическая практика» (посвященной 100-летию

Крымского федерального университета им. В. И. Вернадского) (г. Симферополь-Алушта, 26–27 апреля 2018 г.) / отв. ред. М. А. Михайлов, Т. В. Омельченко; Крымский федеральный университет имени В. И. Вернадского. Симферополь: ИТ «АРИАЛ», 2018. С. 96–98.

5. Руководство пользователя Agisoft Metashape Professional Edition, версия 1.5 // Agisoft: официальный сайт. Дата публикации: 2019. URL: https://www.agisoft.com/pdf/metashape-pro_1_5_ru.pdf.

6. Скрипченко А. В. Техничко-криминалистическая экспертиза документов: учебник / А. В. Скрипченко, Д. С. Коровкин. СПб.: Санкт-Петербургский университет МВД России, 2014. Ч. II. 212 с.

7. Торопова М. В. Криминалистическая экспертиза установления относительной давности выполнения реквизитов документов: дис. ... канд. юрид. наук. Москва, 2014. 202 с.

Viktoriya A. Kuskova

Student,

National Research Lobachevsky State University of Nizhny Novgorod
(Nizhny Novgorod, Russian Federation)
vickus25@mail.ru

Anna. S. Tsibireva

Student,

National Research Lobachevsky State University of Nizhny Novgorod
(Nizhny Novgorod, Russian Federation)
anna.tsibireva.99@mail.ru

Scientific supervisor – A. V. Polyakova, Senior Lecturer of the Department of Forensic Examination

APPLICATION OF THE METHOD OF THREE-DIMENSIONAL MODELING IN PURPOSE OF ESTABLISHING THE CHRONOLOGICAL SEQUENCE OF EXECUTION OF CROSSING STROKES

Abstract: The article considers the possibility of applying the method of three-dimensional modeling in purpose of establishing the relative age of document details. This scientific work is based on the results of a scientific and practical research, in the framework of which was created a 3D models of crossing strokes and examined.

Keywords: establishing the relative age of document details, the crossing strokes, 3D-models, the method of three-dimensional modeling, technical and forensic examination of documents.

УДК 351.74

Полтавский Богдан Сергеевич

Студент,

Елецкий государственный университет им. И. А. Бунина

(г. Елец, Российская Федерация)

leonard9696@mail.ru

Научный руководитель – Е. А. Очеретько, кандидат юридических наук, доцент
кафедры гражданского и предпринимательского права

КАК ТЕХНОЛОГИИ ИЗМЕНЮТ ПОЛИЦЕЙСКУЮ ДЕЯТЕЛЬНОСТЬ

Аннотация: Научно-фантастическое видение полицейских, спешащих на место преступления еще до того, как оно было совершено, может показаться довольно надуманным, но реальность такова, что современные технологии делают это возможным. Использование камер слежения, дронов, роботизация, ведение информационных баз данных и внедрение искусственного интеллекта изменяет образ полицейского, само видение полиции и её деятельности, поэтому необходимо изучить эти процессы и рассмотреть последствия их использования, ввиду огромной значимости органов правопорядка для личности, общества и государства.

Ключевые слова: полиция, правоохранительные органы, общественная безопасность, информационные технологии, цифровизация, базы данных.

Для цитирования:

Полтавский Б. С. Как технологии изменяют полицейскую деятельность // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 497–503.

В современном мире новейшие технические средства очень часто используются для совершения всё большего числа преступлений, поэтому для их предотвращения сотрудникам правоохранительных органов также необходимо использовать достижения науки и техники, чтобы обеспечить общественную, государственную безопасность, а также защитить права и свободы человека. В связи с этим повышаются требования к подготовке и квалификации полицейских,

возникает необходимость в постоянном совершенствовании их навыков и умений. Более того, в условиях цифровизации и роботизации перед правоохранительными органами, как и перед другими профессиями, встаёт вопрос о конкурентоспособности не только между людьми, но и машинами, которые могут заменить человека если не во всей системе, то как минимум в отдельных её отраслях.

Рассмотрим несколько интересных технологий, которые

сегодня играют значительную роль в сфере обеспечения общественной безопасности.

Во-первых, стоит поговорить о ведении полицией баз данных, которые содержат в себе различные сведения, связанные с криминалом. Информация всегда являлась важной частью любой сферы жизни особенно в последние десятилетия в связи с активным использованием интернета. Так, по данным IDC (International Data Corporation) – международно-исследовательская и консалтинговая компания, занимающаяся изучением мирового рынка информационных технологий и телекоммуникаций – в 2020 году во всем мире было сгенерировано около 64,2 зеттабайт данных¹. Для понимания того насколько это колоссальная цифра скажем, что 1 зеттабайт равен примерно 1 триллиону гигабайт. Всё это результат активной информатизации общества и экономики, соответственно полиция учитывает эти тенденции и стремится перевести весь оборот получаемых ими данных с бумажных носителей в фото-, видеофайлы и в различные электронные носители информации, которые хранятся в специализированных банках данных. Особенно это касается документооборота, который пытаются перевести в «цифру» (электронный документооборот). В качестве основных положительных моментов

от внедрения системы электронного документооборота в деятельность отечественной полиции выделяют «ускорение обработки информации внутри ведомства, улучшение и ускорение процесса принятия оперативных решений, повышение их качества, усиление контроля за их выполнением, улучшение взаимодействия и координации непосредственно между подразделениями»².

Часто специалисты правоохранительных органов обращаются к нескольким базам данных, чтобы повысить точность своих расследований. Сбор данных в правоохранительной деятельности помогает специалистам несколькими способами. Например, ДНК и отпечатки пальцев могут храниться в базах данных и использоваться для более быстрой идентификации подозреваемых. Данные также могут помочь правоохранительным органам распознать тенденции преступности и принять соответствующие меры.

Рост баз данных привел к появлению систем быстрой идентификации, которые позволяют полицейским быстро просматривать криминальную историю отдельных лиц с помощью простого поиска. Например, люди, лишённые права управления автомобилем, могут быть быстро идентифицированы с помощью единой базы данных ГИБДД.

¹ Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts // IDC Corporate. URL: <https://www.idc.com/getdoc.jsp?containerId=prUS47560321> (accessed: 16.05.2021).

² Внуков В. И., Непомнящих Д. М. Некоторые вопросы внедрения системы электронного документооборота в органах внутренних дел // Современный ученый. 2017. № 7. С. 300–303.

Системы идентификации нового поколения используют биометрические данные, включая отпечатки пальцев, отпечатки ладоней, распознавание радужной оболочки глаза и лица, чтобы сопоставить людей с их криминальной историей. Современные технологии постоянно обновляются, и добавляются новые, чтобы сделать системы идентификации наиболее полным способом сбора актуальной информации об исследуемом человеке.

Всё это плавно подводит нас к ещё одной технологии, которую активно используют современные полицейские, а именно системы обнаружения, наблюдения, мониторинга и позиционирования.

Сегодня правоохранительные органы могут использовать технологии для обнаружения и раскрытия преступной деятельности, происходящей в данный момент времени, или которая происходила в прошлом. Технологии обнаружения, наблюдения, мониторинга и систем позиционирования, помогают правоохранительным органам в их ежедневной работе. В частности, в последнее время особую роль в работе полиции стали занимать камеры видеонаблюдения, дроны, квадрокоптеры, система НМС и другие подобные технологии. Использование их правоохранительными органами помогает не только обеспечивать оперативное предотвращение преступлений, оптимизацию процессов работы и увеличение

показателей раскрываемости преступлений, но также они могут поспособствовать устранению таких нежелательных инцидентов, как превышение полицейскими должностных полномочий, необоснованное применение силы к невиновным лицам и неадекватное поведение людей в отношении полицейских.

Особо стоит отметить активное использование дорожных камер видеонаблюдения органами ГИБДД начиная с 2006 года, благодаря которым значительно возросло количество штрафов за нарушение ПДД (Правил дорожного движения). По последней статистике только благодаря камерам в 2020 году было вынесено около 145 миллионов штрафов, что на 20 % больше, чем в 2019 году³. В основном штрафы были вынесены за превышение скорости (около 124 миллионов постановлений), дальше идёт несоблюдение требований, предписанных знаками или разметкой (13 миллионов) и проезд на запрещающий сигнал светофора (5 миллионов). Использование подобных камер во многом оказывает психологическое воздействие на потенциальных правонарушителей, поскольку его нарушение не останется незамеченным, и он будет вынужден соблюдать требования закона. Стоит также отметить, что у водителей с 1 сентября 2021 года появится возможность опротестовать штрафы в онлайн режиме через сайт «Госуслуги», что значительно упростит для граждан возможность

³ Буранов И. Камеры принесли 145 млн постановлений // Коммерсантъ. 2021. 15

фев. URL: <https://www.kommersant.ru/doc/4692343> (дата обращения: 16.05.2021).

доказать незаконность полученного ими штрафа и соответственно повысится степень объективности получаемых ГИБДД сведений путём улучшения системы видеонаблюдения.

В последнее время полиция всё активней в своей деятельности применяет такие современные виды техники как беспилотные летательные аппараты (БПЛА), которые используются при необходимости получить вид сверху, т. е. с воздуха на месте происшествия, они могут помочь правоохранительным органам безопасно наблюдать за определенной местностью, предупредить, выявить, пресечь, раскрыть и расследовать преступление. Используя БПЛА при преследовании преступника, пытающегося скрыться от органов правопорядка, оператор может в режиме реального времени передавать оперативной группе полученные им сведения, такие как место нахождения подозреваемого, маршрут его движения и оптимальное место для его задержания. Также при помощи БПЛА может осуществляться и поиск лиц, пропавших без вести или скрывающихся от органов следствия, дознания или суда без необходимости привлечения большой по численности розыскной группы. В целом БПЛА можно охарактеризовать как достаточное эффективное устройство и с дальнейшим усовершенствование подобной техники будет

увеличиваться её роль в работе органов полиции⁴.

Стоит также затронуть вопрос об использовании органами правопорядка камер наблюдения с возможностью биометрического распознавания лица. Данная технология позволяет автоматически идентифицировать человека при помощи нейросети, которая умеет считывать черты человеческого лица проходящих по улице людей и в ту же секунду сравнивать их с фотографиями лиц внесенных в полицейскую или иную базу и находить тем самым преступников или правонарушителей. По сути это искусственный интеллект, который самостоятельно обучается, собирает и анализирует огромные объемы данных в считанные секунды. Активное использование этой системы в России началось не так давно, но определённые результаты её работы уже имеются. Так на Чемпионате Мира по футболу в России 2018 года было задержано около 200 человек при помощи системы распознавания лица. Однако и риски, связанные с её внедрением колоссальны, особенно для обычных граждан⁵.

Теперь поговорим о роли в деятельности полиции навигационно-мониторинговых систем (НМС), основанных на применении глобальных навигационных спутниковых систем. НМС не только

⁴ Косовский В. Б., Мартынюк С. Н. Актуальные вопросы практического применения беспилотной техники в органах внутренних дел Российской Федерации // Общество: политика, экономика, право. 2020. № 3 (80). С. 25–29.

⁵ Зуйкова А. Как работает распознавание лиц и можно ли обмануть эту систему // РБК.Тренды. URL: <https://trends.rbc.ru/trends/industry/6050ac809a794712e5ef39b7> (дата обращения: 16.05.2021).

помогает полицейским легче добраться до места преступления или найти преступников, но и также улучшить управление полицейскими силами, поскольку карты распространения информации о сотрудниках полиции могут обеспечить охват большего числа районов. Интеграция НМС с другими полицейскими системами помогает сделать данные более надежными, поскольку службы определения местоположения легко включаются в отчетность. Камеры наблюдения вместе с НМС могут фиксировать события в определенном районе и предоставлять правоохранительным органам более полную и ценную информацию о преступлении. Таким образом, НМС позволяет: «анализировать результаты работы нарядов, состояние преступности, помогает определять и прогнозировать участки с неблагоприятной криминогенной обстановкой, позволяет вести учет и архивацию информации о передвижении автомобильных патрулей, позволяет осуществлять рациональную корректировку и расстановку сил и средств ОВД»⁶.

Ожидается, что использование роботов для оказания помощи правоохранительным органам будет расти быстрыми темпами в ближайшие годы во всём мире, в том числе и в Российской Федерации. Одной из причин необходимости

«внедрения роботов и робототехнических комплексов в правоохранительной сфере, является насущная потребность в высвобождении человеческих ресурсов от выполнения рутинной и однообразной работы»⁷. Стоит, однако, понимать, что на данный момент времени подобные роботы в большинстве случаев не являются автономными и так или иначе они находятся под управлением человека, и для их функционирования нужна определенная инфраструктура. Поэтому все они выполняют ограниченный набор полицейских функций, например: наблюдение, идентификация, незначительное физическое воздействие на правонарушителя, прием и отправка сообщений и т. д. Соответственно они не обладают теми полномочиями, которые присущи полицейскому (производить задержание, досмотр, оперативно розыскные мероприятия и т. д. без присмотра оператора или полицейского). В Соединенных Штатах роботы обычно используются для разведки в опасных ситуациях и для обезвреживания бомб. В будущем, по мнению американских полицейских, могут появиться охранные роботы, которые будут высматривать подозрительную активность и патрулировать перекрестки. В Дубае, в Объединенных Арабских Эмиратах, полицейские роботы позволяют

⁶ Тарчоков Б. А., Бураева Л. А., Практика использования навигационно-мониторинговых систем подразделениями органов внутренних дел // Проблемы экономики и юридической практики. 2017. № 4. С. 132–134.

⁷ Лукашов Н. В. Организационные и правовые основы применения полицейских робототехнических комплексов в органах внутренних дел российской федерации // Труды Академии управления МВД России. 2020. № 3 (55). С. 210–221.

гражданам задавать им вопросы, оплачивать штрафы и получать доступ к полицейской информации⁸. Однако ещё не в одной стране мира не существует робота-полицейского, который был бы способен полностью заменить на этом посту человека, ввиду относительно слабого уровня развития робототехники.

Таким образом, можно заключить, что технологии уже сейчас играют значительную роль в деятельности полиции. В дальнейшем это влияние будет только расти, поскольку органы внутренних дел, как отечественные, так и зарубежные, сталкиваются каждый день с новыми вызовами, для своевременных решений которых необходимо всегда

соответствовать духу времени. Полиция будущего – это прежде всего новые образовательные инструменты, подходы, способы мышления для обучения соответствующих своей эпохе сотрудников, обладающих квалифицированными профессиональными навыками для решения оперативных задач, способствующих обеспечению общественной безопасности. Полицейский будущего должен быть готов к технологическим вызовам, которые ему бросает новая реальность, даже если ради этого ему придётся претерпеть колоссальные изменения, поскольку без полицейского сложно себе представить общество и государство.

Список литературы

1. Буранов И. Камеры принесли 145 млн постановлений // Коммерсантъ. 2021. 15 фев. URL: <https://www.kommersant.ru/doc/4692343>.
2. Внуков В. И. Некоторые вопросы внедрения системы электронного документооборота в органах внутренних дел / В. И. Внуков, Д. М. Непомнящих // Современный ученый. 2017. № 7. С. 300–303.
3. Зуйкова А. Как работает распознавание лиц и можно ли обмануть эту систему // РБК.Тренды. URL: <https://trends.rbc.ru/trends/industry/6050ac809a794712e5ef39b7>.
4. Косовский В. Б. Актуальные вопросы практического применения беспилотной техники в органах внутренних дел Российской Федерации / В. Б. Косовский, С. Н. Мартынюк // Общество: политика, экономика, право. 2020. № 3 (80). С. 25–29.
5. Лукашов Н. В. Организационные и правовые основы применения полицейских робототехнических комплексов в органах внутренних дел российской федерации // Труды Академии управления МВД России. 2020. № 3 (55). С. 210–221.
6. Тарчоков Б. А. Практика использования навигационно-мониторинговых систем подразделениями органов внутренних дел / Б. А. Тарчоков, Л. А. Бураева // Проблемы экономики и юридической практики. 2017. № 4. С. 132–134.

⁸ Page T. The inevitable rise of the robocops // CNN. URL: <https://edition.cnn.com/2017/05/2>

<2/tech/robot-police-officer-future-dubai/index.html> (accessed: 16.05.2021).

7. Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts. // IDC Corporate. URL: <https://www.idc.com/getdoc.jsp?containerId=prUS47560321>.

8. Page T. The inevitable rise of the robocops // CNN. URL: <https://edition.cnn.com/2017/05/22/tech/robot-police-officer-future-dubai/index.html>.

Bogdan S. Poltavsky

Student,

Yelets State University named after I. A. Bunina

(Yelets, Russian Federation)

leonard9696@mail.ru

Scientific supervisor – E. A. Ocheretko, PhD (Law), Associate Professor of the
Department of Civil and Business Law

HOW TECHNOLOGY WILL CHANGE POLICE ACTIVITIES

Abstract: The sci-fi vision of police officers rushing to the scene of a crime before it has even been committed may seem rather far-fetched, but the reality is that modern technology makes it possible. The use of security cameras, drones, robotics, maintaining information databases and the introduction of artificial intelligence changes the image of the police, the very vision of the police and its activities, so it is necessary to study these processes and consider the consequences of their use, given the enormous importance of law enforcement bodies for the individual, society and the state.

Keywords: police, law enforcement, public security, information technology, digitalization, databases.

Темирова Алина Ильдаровна

Студент,

Южно-Уральский государственный университет
(Национальный исследовательский университет)

(г. Челябинск, Российская Федерация)

alina.temirova.99@mail.ru

Научный руководитель – Т. И. Ястребова, кандидат юридических наук, доцент
кафедры уголовного процесса, криминалистики и судебной экспертизы

К ВОПРОСУ ОБ ОСОБЕННОСТЯХ ОРГАНИЗАЦИИ РАССЛЕДОВАНИЙ ПРЕСТУПЛЕНИЙ «ПО ГОРЯЧИМ СЛЕДАМ»

Аннотация: В статье автор рассматривает сущность такого понятия, как «расследование преступления по горячим следам», а также исследует наиболее распространенные сложности, с которыми на практике сталкиваются сотрудники правоохранительных органов. Рассматривается значение тактических операций для решения указанной проблемы.

Ключевые слова: расследование, следственно-оперативная группа, по горячим следам, время, преступление, взаимодействие, тактика, поиск.

Для цитирования:

Темирова А. И. К вопросу об особенностях организации расследований преступлений «по горячим следам» // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 504–508.

Ключевой задачей, стоящей перед органами предварительного расследования, выступает расследование и раскрытие преступлений, эффективность которых зависит не только от профессионализма сотрудников, но и от своевременного прибытия следственно-оперативной группы (далее – СОГ) к месту происшествия. Только оперативное реагирование сотрудников полиции на совершенное преступление и незамедлительное прибытие СОГ на место позволят установить наиболее полный объем информации, который в дальнейшем

позволит выявить лиц, совершивших преступное деяние, а также раскрыть преступление «по горячим следам». Раскрытие преступления «по горячим следам» выступает наиболее эффективным, поскольку сотрудники правоохранительных органов владеют актуальной информацией о преступном посягательстве, обладают возможностью исследовать следы, установить очевидцев произошедшего, задержать подозреваемого в первые сутки.

В современных условиях сложившаяся криминальная ситуация характеризуется наличием широкого

круга негативных криминалистически значимых фоновых проявлений преступности, которые создают существенные препятствия успешному проведению первоначальных следственных действий, в том числе, раскрытию преступления «по горячим следам»¹. Кроме того, на участников СОГ возлагается обязанность проводить расследование в максимально короткие сроки с применением эффективных и результативных методик, средств и способов. Каждая ошибка, совершенная сотрудниками правоохранительных органов, создает для преступников дополнительную возможность скрыться от правосудия. В связи с этим, представляют большую значимость теоретические и научные разработки проблем расследования преступления, что призвано повысить эффективность следственной деятельности.

Научные положения, ведомственные нормативные акты не сформировали единообразный подход к пониманию такой категории, как раскрытие преступлений «по горячим следам». Так, Н. П. Яблоков указывал, что сроки расследования «по горячим следам» исчисляются 5 днями². Некоторые ученые, в том числе В. П.

Лавров, В. Е. Сидоров указывали, что данный период может быть продлен до 10–15 суток³. В то же время Р. С. Белкин считает, что раскрытие преступления «по горячим следам» предусматривает расследование в максимально сжатые сроки, то есть за трое суток с момента получения сообщения о посягательстве, в исключительных случаях срок может быть увеличен до 10–15 суток⁴. На уровне правового регулирования закреплены следующие временные рамки расследования преступлений «по горячим следам». В многостороннем приказе «О едином учете преступлений» от 29.12.2005, а именно, в приложении № 4, приведена форма № 1 «Статистическая карточка на выявленное преступление», в которой отдельным положением выделено установление подозреваемого в течение 24 часов после регистрации сообщения о преступлении. Вместе с этим, Инструкция о порядке заполнения и представления необходимых учетных данных устанавливает, что соответствующий код в карточке формы № 1 заполняется только в том случае, если сотрудниками преступление было расследовано «по горячим следам»⁵.

¹ Тепляшин П. В. Тенденции преступности в Сибирском федеральном округе (глубина анализа 6 лет) // Деятельность правоохранительных органов в современных условиях. 2019. № 1. С. 92–94.

² Яблоков Н. П. Криминалистика: учебник и практикум для бакалавриата и специалитета. 3-е изд., перераб. и доп. М.: Изд-во Юрайт, 2019. С. 239.

³ Лавров В. П., Сидоров В. Е. Расследование преступлений по горячим следам: учебное пособие. М. 1999. С. 85.

⁴ Криминалистика: учебник для вузов / Р. С. Белкин, Т. В. Аверьянова, Ю. Г. Корухов, Е. Р. Россинская. М.: НОРМА, 2001. С. 854.

⁵ О едином учете преступлений: приказ Генпрокуратуры России № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 (ред. от 15.10.2019) (вместе с «Типовым положением о едином порядке организации приема, регистрации и проверки сообщений о

Считаем, что подход законодателя к определению сущности расследования преступлений «по горячим следам», не учитывает специфику расследования отдельных категорий преступлений. Так, по экономическим преступлениям оперативная работа нередко реализуется в течение нескольких месяцев, после чего должностное лицо составляет рапорт об обнаружении признаков преступления, на основании которого делается регистрационная запись в КУСП. В сложившейся ситуации говорить о раскрытии преступления «по горячим следам» нерационально. Полагаем необходимым рассматриваемую категорию применять только по отношению к преступлениям общеуголовной направленности. В Приказ «О едином учете преступлений» следует включить дополнение, а именно, в п. 5 Приложения № 1 в следующем виде: «Преступление является раскрытым «по горячим следам» в том случае, если по результатам проведенной проверки сообщения о совершенном преступлении или с момента обнаружения признаков преступления, в течение 24 часов с момента регистрации соответствующей записи в КУСП сотрудниками установлено лицо, в

отношении которого в дальнейшем возбуждено уголовное дело».

Анализ практики и многочисленные исследования в области расследования преступлений «по горячим следам», указывают на возникновения ряда сложностей перед сотрудниками правоохранительных органов: дефицит времени и информации, отсутствие налаженного взаимодействия между сотрудниками различных подразделений ОВД, производство отдельных следственных действий (отсутствие системности и последовательности)⁶. Нейтрализация негативного воздействия рассматриваемых факторов на деятельность участников СОГ, в большей степени достигается посредством использования метода тактических операций. Под тактическими операциями понимаются инструменты разрешения общих задач предварительного расследования посредством производства не разрозненных следственных действий, а системы мероприятий, в структуру которых будут включаться как оперативно-розыскные, а так и ревизионные операции⁷. Только при помощи тактических операций и налаженного взаимодействия следователя с сотрудниками оперативных подразделений, участковыми

преступлениях», «Положением о едином порядке регистрации уголовных дел и учета преступлений», «Инструкцией о порядке заполнения и представления учетных документов») // СПС «КонсультантПлюс». URL:

http://www.consultant.ru/document/cons_doc_LAW_57951/ (дата обращения: 15.05.2021).

⁶ Уварова А. В. Раскрытие преступления «по горячим следам»: проблемы формулировки и

нормативного закрепления // Правовая система и современное государство: проблемы, тенденции и перспективы развития. 2020. № 1. С. 143–145.

⁷ Рогова И. Г., Пятибратов В. А. Проблемы и особенности расследования преступлений по горячим следам // Международный журнал гуманитарных и естественных наук. 2018. № 6-2. С. 135–139.

уполномоченными полицией и экспертами, в максимально короткий срок может быть найдено похищенное имущество, задержан подозреваемый, либо проведено задержание с поличным, найдены и зафиксированы следы преступления, изобличены виновные лица.

Подводя итог вышесказанному, следует отметить, что в настоящее время на уровне межведомственного приказа не закреплено полноценное понятие «расследование по горячим следам», что на наш взгляд негативно

сказывается на практике. В связи с этим, целесообразно включить соответствующие изменения в Приказ «О едином учете преступлений». Кроме того, эффективность расследования «по горячим следам» достигается посредством преодоления сложностей организационного характера, поскольку только в условиях налаженного взаимодействия, реализации совместных мероприятий, можно говорить об результативной работе.

Список литературы

1. Криминалистика: учебник для вузов / Р. С. Белкин, Т. В. Аверьянова, Ю. Г. Корухов, Е. Р. Россинская. М.: НОРМА, 2001.
2. Лавров В. П. Расследование преступлений по горячим следам: учебное пособие / В. П. Лавров, В. Е. Сидоров. М. 1999.
3. Рогава И. Г. Проблемы и особенности расследования преступлений по горячим следам / И. Г. Рогава, В. А. Пятибратов // Международный журнал гуманитарных и естественных наук. 2018. № 6-2. С. 135–139.
4. Тепляшин П. В. Тенденции преступности в Сибирском федеральном округе (глубина анализа 6 лет) // Деятельность правоохранительных органов в современных условиях. 2019. № 1. С. 92–94.
5. Уварова А. В. Раскрытие преступления «по горячим следам»: проблемы формулировки и нормативного закрепления // Правовая система и современное государство: проблемы, тенденции и перспективы развития. 2020. № 1. С. 143–145.
6. Яблоков Н. П. Криминалистика: учебник и практикум для бакалавриата и специалитета. 3-е изд., перераб. и доп. М.: Изд-во Юрайт, 2019.

Alina I. Temirova

Student,

South Ural State University
(National Research University)
(Chelyabinsk, Russian Federation)
alina.temirova.99@mail.ru

Scientific supervisor – T. I. Yastrebova, PhD (Law), Associate Professor of the
Department of Criminal Process, Forensics and Forensic Expertise

TO THE QUESTION ABOUT THE SPECIFIC FEATURES OF THE ORGANIZATION OF CRIME INVESTIGATIONS «ON HOT PURSUIT»

Abstract: In the article, the author examines the essence of such a concept as «hot pursuit of a crime» and also examines the most common difficulties that law enforcement officers face in practice. The importance of tactical operations for solving this problem is considered.

Keywords: investigation, investigative-operational group, hot pursuit, time, crime, interaction, tactics, search.

УДК 343.98

Шабунина Елизавета Алексеевна
Заместитель командира взвода (курсант),
Санкт-Петербургский университет МВД России
(г. Санкт-Петербург, Российская Федерация)
shabunina95@yandex.ru

Научный руководитель – Е. Ю. Родина, старший преподаватель кафедры
криминалистики

ЭКСПЕРТНЫЕ ОШИБКИ ПРИ ДНК-ИДЕНТИФИКАЦИИ: ВИДЫ, ПРИЧИНЫ, ЗНАЧЕНИЕ

Аннотация: В статье затронута проблема возникновения экспертных ошибок при работе с объектами биологического происхождения, являющимися потенциальными вещественными доказательствами по уголовному делу. Автор обращает внимание на причины процессуального и методического характера, являющиеся первоочередными источниками экспертных ошибок при ДНК-идентификации. Доверие методике ДНК-анализа является бесспорным, однако же, результат исследования в первую очередь зависит от подготовки эксперта и соблюдения им условий работы с рассматриваемыми объектами.

Ключевые слова: ДНК-идентификация, ДНК-анализ, биологический след, контаминация, экспертная ошибка.

Для цитирования:

Шабунина Е. А. Экспертные ошибки при днк-идентификации: виды, причины, значение // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 509–514.

Объекты биологического происхождения, обнаруженные на месте происшествия и подвергающиеся впоследствии исследованию при помощи ряда судебных экспертиз, зачастую играют немаловажную роль в формировании доказательственной базы по уголовным делам. Как правило, исследование данных объектов чаще всего проводится по тяжким и особо тяжким преступлениям – убийствам, причинению тяжкого вреда здоровью, изнасилованиям и др.

Разработка новых методов идентификации человека всегда оставалась наиболее актуальной среди задач криминалистики. Уникальность и неповторимость генетических формул человечества позволили разработать экспертную технологию ДНК-идентификации, впоследствии именуемую как «Золотой стандарт» судебной экспертизы. И. О. Перепечина, исследуя генезис становления и развития данной технологии, не раз отмечала, что рассматриваемый метод берёт своё

начало в 1985 году и является достаточно молодым. Считается, что научная база и практическое использование ДНК-анализа разработано гораздо лучше, чем многие другие традиционные методы судебной экспертизы.

Однако следует понимать, что, не смотря на высокий уровень развития современной науки, допущение различного рода экспертных ошибок невозможно исключить. Во-первых, это обусловлено полнотой содержания разработанных на сегодняшний день методик. Практически любой метод может иметь такие грани своего применения, которые попросту не входят в используемые методики.

Во-вторых, поле исследовательской деятельности также влияет на возможность возникновения ошибочного суждения. Диапазон, в котором применение метода даёт достоверные результаты, должен строго соблюдаться. На практике многие эксперты пренебрегают данным требованием.

В-третьих, отсутствие ошибок может быть гарантировано только при безупречном выполнении метода, что во многом зависит от практического опыта эксперта.

Рассматриваемая проблематика носит не только сугубо научно-методический характер, но и затрагивает такие проблемы, как правовое регулирование экспертной деятельности в России, несовершенство уголовно-

процессуальной деятельности, пробелы в программах подготовки судебно-экспертных кадров. Проанализируем возможные причины экспертных ошибок, имеющие как методический, так и процессуальный характер.

1. Причины экспертных ошибок процессуального характера.

Во-первых, следует обратить первоочередное внимание на сохранность объектов, представленных на исследование. В результате нарушений условий хранения, биологические объекты меняют свои свойства, что в последующем отражается на полученных результатах исследования. Приведём следующий пример: при хранении образцов крови был нарушен температурный режим, в результате чего произошло развитие гнилостных изменений, что повлекло за собой бактериальное загрязнение объекта и деградацию ДНК¹. Результат такого исследования нельзя считать достоверным.

Во-вторых, научно разработанная последовательность идентификационного исследования требует предварительного изучения природы представленного следа. То есть, исследование ДНК без предварительной судебно-биологической экспертизы является недопустимым. Данное положение затрагивает как экспертную, так и следственную практику в части, касающейся описания объектов, представленных на исследование².

¹ Барыгина А. А., Старикова И. Л. Оценка допустимости и достоверности заключений судебно-медицинских экспертиз // Вестник ЮУрГУ. Серия: Право. 2017. № 2. С. 13–16.

² Перепечина И. О. Криминалистическая идентификация человека на основе его генетических свойств: (избранные труды): [в 5 т.] Т. 4: Криминалистическая ДНК-

Например, использование следователем дефиниции «пятно крови» в постановлении о назначении экспертизы не является для эксперта основанием для пропуска этапа установления биологической природы объекта. Более того, следователь не вправе давать оценочные суждения касательно исследуемых объектов, что является юридически недопустимым.

2. Методические причины экспертных ошибок.

Данная категория ошибок заключается в выборе экспертом не оптимальной для того или иного конкретного случая методики исследования, либо в нарушении правил или принципов данного вида исследования. При этом необходимо учитывать следующие наиболее распространённые факторы, оказывающие влияние на появление экспертной ошибки.

Малое количество исследуемого биологического материала: данный фактор наиболее актуален при использовании иммунологических методов, направленных на выявление соответствующего антигена. Недостаточность количества материала сказывается на сложности выявления его слабой формы и приводит к ошибке в установлении групповой принадлежности объекта (Пример: ошибки в определении групповой принадлежности крови).

регистрация; Ошибки при ДНК-идентификации и их предотвращение; Криминалистическое ДНК-фенотипирование. 2015. 376 с.

³ Фирсов О. А., Волков А. С. Особенности обнаружения и изъятия следов биологического происхождения при раскрытии и расследовании преступлений // Вестник Саратовского государственного

Деграция ДНК: данное явление обуславливается негативным воздействием внешней среды. Например, использование источников ультрафиолетового излучения при осмотре места происшествия приводит к видоизменению биологических свойств следов. В связи с чем, О. А. Фирсов в своё время предположил целесообразность использования источников ультрафиолетового излучения с более длинноволновым спектром УФ-излучения, а также необходимость сокращения до минимума времени облучения участков местности³.

В 2017 году группа учёных под руководством Т. Г. Фалеевой провела практический эксперимент, заключающийся в изучении деграции ДНК с течением времени в смывах, выполненных при помощи деионизированной воды. Полученный результат позволил судить о существенном уменьшении концентрации ДНК: более чем в 20 раз спустя 5–7 суток и в 179 раз спустя 30 суток⁴. Данное положение актуально и для вышеприведённого фактора.

«Смешанный» характер объекта. Зачастую объектами исследования становятся следы, содержащие биологический материал разных индивидуумов, либо биологический материал разной природы одного индивидуума

социально-экономического университета. 2013. № 5 (49). С. 165–167.

⁴ Деграция ДНК в смывах с течением времени / Т. Г. Фалеева, И. Н. Иванов, Е. С. Мишин, И. В. Корниенко // Молекулярная диагностика: сборник трудов IX Всероссийской научно-практической конференции с международным участием. 2017. С. 413–414.

(например, кровь и выделения). Такое смешение значительно затрудняет интерпретацию получаемых результатов и представляет собой крайне сложную задачу в ДНК-анализе, поскольку не всегда имеется информация касательно числа лиц, ДНК которых содержится в объекте, ни сам факт наличия смеси. В данном контексте весьма эффективна методика так называемого «дифференциального лизиса», позволяющая отделить, к примеру, ДНК семенной жидкости от ДНК иной природы (например, крови) и получить «чистые» профили соответствующей ДНК.

Контаминация (от англ. – загрязнение): наиболее распространённый негативный фактор, оказывающий влияние на подавляющее большинство экспертных ошибок. Загрязнение может произойти на каждом этапе манипуляций с исследуемыми объектами. Зачастую контаминация происходит на этапе изъятия объектов с места происшествия в виду несоблюдения мер предосторожности. Например, загрязнение изымаемых объектов может возникнуть из-за отсутствия надлежащей обработки инструментов после работы с каждым объектом; в виду помещения изъятых объектов в одну и ту же упаковку и др.

Однако наиболее распространённой проблемой в данном контексте является контаминация при нарушении правил проведения экспертных исследований при ДНК-анализе, производимых в лабораториях.

Таким образом, анализ рассмотренных процессуальных

нарушений и факторов, порождающих экспертные ошибки, позволяет прийти к следующему выводу. Заключение, получаемые на основе ошибочных экспертных исследований и используемые при дальнейшей ДНК-идентификации, ведут к возникновению следующих ситуаций:

1. исключение возможности происхождения объекта от проходящего по уголовному делу лица;

2. совпадение неправильно определённого профиля ДНК с одним из профилей, содержащихся в базе данных.

Данные ситуации, с нашей точки зрения, оказывают сильнейшее негативное влияние на ход следствия. В первом случае, экспертная ошибка ведёт к направлению расследования по ложному пути, а также исключению блока доказательств.

Вторая приведённая ситуация может породить гораздо более серьёзные последствия, а именно – привлечение к уголовной ответственности невиновного. Истории известны случаи, когда экспертные ошибки выявлялись исключительно благодаря наличию твёрдого алиби у подозреваемых субъектов, которые в силу возраста или физических особенностей попросту не могли совершить преступление.

Практика предупреждения экспертных ошибок на сегодняшний день достигается путём прокурорского надзора и внутриведомственного контроля за экспертной деятельностью в системе МВД России. Так, данная контрольно-надзорная деятельность

регламентируется следующими нормативными источниками:

1. Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации»;

2. Наставление по организации экспертно-криминалистической деятельности в системе Министерства внутренних дел Российской Федерации, утвержденное Приказом МВД России от 11.01.2009 № 7;

3. Приказ Министерства внутренних дел Российской Федерации от 29.06.2005 № 511 (в ред. от 27.06.2019) «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», утвердивший инструкцию по организации производства судебных

экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации и Перечень родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации.

Таким образом, необходимо отметить, что предупреждение экспертных ошибок при ДНК-идентификации должно являться одной из первоочередных задач при проведении ДНК-исследований. Комплексный характер мер, осуществляемых при решении данной задачи, включает в себя не только правовой механизм контроля, но и введение повсеместной практики выступления в суде экспертов с обеих сторон процесса для убеждения участников судопроизводства в своей правоте⁵.

Список литературы

1. Барыгина А. А. Оценка допустимости и достоверности заключений судебно-медицинских экспертиз / А. А. Барыгина, И. Л. Старикова // Вестник ЮУрГУ. Серия: Право. 2017. №2. С. 13–16.

2. Деграция ДНК в смывах с течением времени / Т. Г. Фалеева, И. Н. Иванов, Е. С. Мишин, И. В. Корниенко // Молекулярная диагностика: сборник трудов IX Всероссийской научно-практической конференции с международным участием. 2017. С. 413–414.

3. Перепечина И. О. Криминалистическая идентификация человека на основе его генетических свойств: (избранные труды): [в 5 т.]. Т. 4: Криминалистическая ДНК-регистрация; Ошибки при ДНК-идентификации и их предотвращение; Криминалистическое ДНК-фенотипирование. 2015. 376 с.

4. Фирсов О. А. Особенности обнаружения и изъятия следов биологического происхождения при раскрытии и расследовании преступлений / О. А. Фирсов, А. С. Волков // Вестник Саратовского государственного социально-экономического университета. 2013. № 5 (49). С. 165–167.

⁵ Ярмач К. В. Пути предупреждения экспертных ошибок // Деятельность правоохранительных органов в современных

условиях: сборник материалов 20-й международной научно-практической конференции. 2015. С. 40–44.

5. Ярмак К. В. Пути предупреждения экспертных ошибок // Деятельность правоохранительных органов в современных условиях: сборник материалов 20-й международной научно-практической конференции. 2015. С. 40–44.

Elizaveta A. Shabunina

Cadet,

St. Petersburg University of the Ministry of Internal Affairs of Russia
(Saint Petersburg, Russian Federation)
shabunina95@yandex.ru

Scientific supervisor – E. Yu. Rodina, Senior Lecturer of the Department of
Criminalistics

THE EXPERT'S MISTAKES FOR DNA IDENTIFICATION: TYPES, CAUSES, SIGNIFICANCE

Abstract: In the article the author deals with the problem of the occurrence of expert mistakes during working with objects of biological origin which are potential material evidence in a criminal case. The author matches attention to the reasons of a procedural and methodological nature which are the primary sources of expert mistakes in DNA identification. Confidence in the method of DNA analysis is indisputable; however, the result of the examination primarily depends on the training of the expert and compliance with the conditions for working with the objects under consideration.

Keywords: DNA identification, DNA analysis, biological trace, contamination, expert mistake.

УДК 342.5

Эмирбеков Фарид Язибекович

Студент,

Уральский государственный юридический университет

(г. Екатеринбург, Российская Федерация)

emirbekov.farid00@mail.ru

Научный руководитель – М. В. Гончаров, кандидат юридических наук, доцент
кафедры конституционного права

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В СЛЕДСТВЕННОМ КОМИТЕТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: В данной статье исследуются проблемы использования электронного документооборота в деятельности Следственного комитета Российской Федерации по расследованию уголовных дел. Анализируются основные функции цифровых технологий, применяемых при составлении процессуальных и иных следственных документов. Делается вывод, что применение информационных технологий и разработка единой автоматизированной системы делопроизводства и электронного документооборота в Следственном комитете Российской Федерации сможет существенно повысить эффективность производства следственных действий.

Ключевые слова: следственный комитет, расследование уголовных дел, делопроизводство, электронный документооборот, автоматизированные информационные системы, искусственный интеллект.

Для цитирования:

Эмирбеков Ф. Я. Проблемы и перспективы использования электронного документооборота в Следственном комитете Российской Федерации // Технологии XXI века в юриспруденции: мат-лы Третьей междунар. науч.-практ. конф. (Екатеринбург, 21 мая 2021 года) / отв. ред. Д. В. Бахтеев. Екатеринбург: Уральский государственный юридический университет, 2021. С. 515–522.

Согласно ст. 1 Федерального закона от 28 декабря 2010 г. № 403-ФЗ «О Следственном комитете Российской Федерации» Следственный комитет России является федеральным государственным органом,

осуществляющим в соответствии с законодательством Российской Федерации полномочия в сфере уголовного судопроизводства¹. Данный орган был создан на базе Следственного комитета при прокуратуре Российской Федерации и

¹ О Следственном комитете Российской Федерации: федер. закон № 403-ФЗ от 28.12.2010: [в ред. от 27.12.2019] // Собрание

законодательства Российской Федерации. 2011. № 1. Ст. 15.

начал осуществлять свою деятельность с 15 января 2011 г.

Выделение Следственного комитета из прокуратуры произошло в целях обеспечения независимости предварительного следствия. В нем предусмотрены следующие виды государственной службы: военная, правоохранительная и федеральная гражданская².

Следственный комитет России в рамках своей деятельности уполномочен решать следующие задачи:

- осуществлять производство качественного и оперативного расследования преступлений;
- контролировать выполнение должностными лицами органов Следственного комитета возложенных на них обязанностей;
- организовывать работу по выявлению факторов, способствующих совершению преступлений, и принимать меры по их устранению;
- реализовывать государственную политику в сфере уголовного судопроизводства;
- разрабатывать направления по совершенствованию нормативно-правового регулирования в сфере уголовного судопроизводства;
- формировать статистическую отчетность деятельности следственных органов.

В соответствии со ст. 12 Федерального закона от 28 декабря 2010 г. № 403-ФЗ «О Следственном

комитете Российской Федерации» в систему Следственного комитета входят:

1. центральный аппарат Следственного комитета Российской Федерации;
2. главные следственные управления и следственные управления Следственного комитета по субъектам Российской Федерации, а также приравненные к ним специализированные следственные управления и следственные отделы Следственного комитета;
3. следственные отделы и следственные отделения Следственного комитета по районам, городам и приравненные к ним, включая специализированные (в том числе военные) следственные подразделения Следственного комитета;
4. криминалистические подразделения Следственного комитета.

В 2020 г. в Российской Федерации было зарегистрировано 2 044 221 преступлений, из них 21 517 выявлено сотрудниками Следственного комитета Российской Федерации. Количество преступлений, уголовные дела по которым предварительно расследованы сотрудниками Следственного комитета Российской Федерации, составило 142 800³. Это является серьезным показателем служебной деятельности Следственного комитета России,

² Абдуллатипова К. А. Проблемы правового статуса Следственного комитета Российской Федерации // Закон и право. 2018. № 11. С. 39.

³ Состояние преступности в России за январь–декабрь 2020 г. // Министерство внутренних дел РФ: официальный сайт. URL: <https://мвд.рф/reports/item/22678184/> (дата обращения: 25.04.2020).

поскольку следователи данного правоохранительного органа расследуют наиболее резонансные преступления в отличие от следователей, входящих в систему Министерства внутренних дел Российской Федерации.

Так, Следственный комитет России уполномочен расследовать отдельные тяжкие и особо тяжкие преступления, совершаемые организованными группами и преступными сообществами, обладающими повышенной степенью общественной опасности⁴. Кроме того, следователи Следственного комитета нередко сталкиваются с противодействием расследованию, признаваемым в последние годы трудноразрешимой проблемой⁵, и обеспечивают наиболее эффективную защиту участников уголовного судопроизводства от преступных посягательств⁶.

В Следственном комитете Российской Федерации большое внимание уделяется документационному обеспечению. Так, Приказом Следственного комитета России от 18 июля 2012 г. № 40 утверждена Инструкция по делопроизводству Следственного комитета, в которой устанавливаются

единые требования по обработке, использованию и хранению документов⁷.

Ни для кого не является секретом, что в Следственном комитете Российской Федерации автоматизация процедур делопроизводства непосредственно влияет не только на оперативность и качество рассмотрения заявлений, жалоб и иных обращений граждан, но и на эффективность расследования преступлений. Проведение отдельных следственных мероприятий в электронном виде позволяет решить целый ряд задач, которые способствуют:

- оптимизации работы следователя;
- удаленному взаимодействию между участниками уголовного судопроизводства;
- усилению гарантий по соблюдению правового статуса личности;
- повышению эффективности прокурорского надзора.

Думается, что для плодотворного решения данных задач необходимо наличие соответствующей программной платформы, которая позволит загрузить имеющиеся материалы

⁴ Яшин А. В. Некоторые проблемы предупреждения преступлений, совершаемых организованными группами или преступными сообществами // Наука. Общество. Государство. 2016. № 1. С. 62.

⁵ Яшин А. В. История развития законодательства об уголовной ответственности за преступления против участников уголовного судопроизводства // Современное право. 2011. № 9. С. 157.

⁶ Яшин А. В. Криминологические особенности системы преступлений против

участников уголовного судопроизводства // Пробелы в российском законодательстве. 2010. № 2. С. 237.

⁷ Об утверждении Инструкции по делопроизводству Следственного комитета Российской Федерации: приказ Следственного комитета Российской Федерации № 40 от 18.07.2012 // СПС «КонсультантПлюс».

URL://www.consultant.ru (дата обращения: 25.04.2020).

уголовных дел, находящихся в производстве следователей, и предоставит возможность их пополнения в случае производства новых процессуальных действий. При всем этом данная система должна иметь уровневый доступ для лиц, как фигурирующих в деле, так и осуществляющих контроль и надзор за предварительным следствием.

В качестве системы электронного документооборота в Следственном комитете Российской Федерации используется автоматизированный информационный комплекс «Надзор». Он оказывает помощь в осуществлении регистрации внутренних, а также входящих и исходящих документов, выполняя тем самым функции электронной картотеки. Однако не следует забывать о том, что основные документы, напрямую относящиеся к расследованию преступлений, имеют ограниченный доступ. Таким образом, должны учитываться все требования к информационным системам для обеспечения безопасности при автоматизации процедур делопроизводства. Иными словами, в основу решения данной задачи должно быть положено построение эффективной автоматизированной системы ограничения доступа. Следует также отметить, что АИК «Надзор» не обладает функциями по применению электронной подписи и не предназначен для работы с конфиденциальной информацией⁸.

Таким образом, АИК «Надзор» не способен в полном объеме обеспечить необходимый документооборот Следственного комитета России.

В АИК «Надзор» автоматизированы только основные стадии работы с документом, а такие сопутствующие процедуры, такие как доведение до сведения, создание проекта документа, принятие решения, согласование, ознакомление, визирование, осуществляются только в бумажном варианте. Все это приводит к дополнительным затратам людских ресурсов и расходных материалов. В ходе эксплуатации АИК «Надзор» было выявлено, что нет единой системы кодирования и классификации информации для Следственного комитета России. Данное обстоятельство во многом затрудняет формирование базы нормативно-справочной информации, в результате чего оптимальная нормативно-правовая база по созданию и использованию электронных документов для работы Следственного комитета России в настоящее время не разработана. И каждая подсистема Следственного комитета вынуждена использовать дополнительное программное обеспечение, оптимизирующее документооборот.

Так, в Следственном комитете используется автоматизированная система уголовно-правовой статистики (АС УПС СКР), оказывающая помощь в выполнении повседневной следственной

⁸ Багмет А. М. Проблемы обеспечения межведомственного электронного документооборота Следственного комитета Российской Федерации с федеральными

государственными органами в сфере уголовного судопроизводства // Правопорядок: история, теория, практика. 2018. № 4. С. 47.

деятельности. Посредством ее применения создаются базы документов, которые во многом облегчают работу сотрудников.

АС УПС СКР предназначена:

- для учета уголовных дел, сообщений о преступлениях, криминалистических характеристик, судебных экспертиз;
- для сбора статистической отчетности и формирования базы статистических данных.

Аналогичное назначение имеет и информационная система «Электронный паспорт уголовного дела». В качестве основных преимуществ данной системы выступают:

1. эффективность процессуального контроля;
2. идентификация процессуальных сроков уголовных дел;
3. учет переквалификаций преступных деяний по уголовным делам.

Несмотря на то, что эти две системы являются составными частями проектируемого автоматизированного комплекса Следственного комитета Российской Федерации, используются они довольно ограниченно. Это связано с тем, что им присущи определенные недостатки, связанные с отсутствием реагирования на изменение следственной ситуации по уголовным делам. В свою очередь системы электронного документооборота Следственного комитета должны обеспечивать непрерывный доступ к

документальной информации на всех уровнях управления⁹.

Помимо указанных выше существует еще множество различных систем электронного документооборота, но их использование в рамках государственной деятельности является нежелательным, поскольку они пока не входят в реестр российского программного обеспечения. Из известных систем электронного документооборота необходимыми функциями располагают такие системы, как «Дело», «Тезис», «Логика ЕСМ», в связи с чем их платформы могут быть использованы для производства отдельных процессуальных и организационных действий в электронной форме.

Например, система электронного документооборота «Дело» предоставляет возможность хранения документов и одновременной работы с ними, что позволяет готовить проекты документов с возможностью их редактирования, согласования и утверждения. Кроме того, интерфейс анализируемой системы оказывает помощь при осуществлении обмена документами с другими базами данных.

В таких системах, как «Дело», «Тезис», «Логика ЕСМ», присутствует возможность разграничения доступа и использования электронной подписи. Данные системы способны дорабатываться под нужды организации-заказчика. Используя их,

⁹ Бычков В. В. Электронный документооборот в следственной деятельности: проблемы и пути их решения /

В. В. Бычков, С. Б. Вепрев // Правопорядок: история, теория, практика. 2018. № 4. С. 51.

следователь получает возможность более оперативно готовить процессуальные документы, пользуясь имеющимися формами, делать копии, вносить поправки при выявлении ошибок технического характера. Посредством данных систем может быть ускорен и процесс ходатайства перед судом о применении отдельных мер пресечения¹⁰.

На мой взгляд, в ходе производства по уголовным делам цифровые технологии позволяют выполнять коммуникативную, доказательственную и интеллектуальную функции.

Так, цифровая форма представления информации способствует более эффективному обмену данными между субъектами уголовного процесса. Расследование электронного дела упрощает участникам уголовного процесса процедуру ознакомления с материалами. Вследствие этого происходит ускорение расследования и рассмотрения уголовного дела. Также введение электронного документооборота в практику позволит увеличить степень «прозрачности» уголовного судопроизводства и обеспечить «разумный» компромисс в борьбе с преступностью¹¹.

В настоящее время уведомление участников процесса о производстве следственных действий осуществляется путем телефонных

звонков и вызова их в кабинет следователя, а ответы на запросы, направляемые почтой, часто приходят в неактуальный срок. Возникают и такие ситуации, когда потерпевшие не могут получить информацию о том, у какого следователя в производстве находится дело по их заявлению. Использование автоматизированных систем смогло бы разрешить указанные проблемы.

Поскольку отечественное уголовно-процессуальное законодательство запрещает разглашение данных предварительного расследования, система электронного документооборота должна предусматривать ограниченный доступ только тем лицам, которые должны проходить процедуру ознакомления с уголовным делом. Предоставление доступа к электронному уголовному делу помогло бы свести к минимуму злоупотребление правом ознакомления с уголовным делом, которым пользуются стороны после окончания предварительного следствия. Наличие электронного уголовного дела также смогло бы решить проблему нецелесообразной траты времени адвокатами на выписывание, фотографирование, согласование со следователем графика ознакомления и т. п.

В настоящее время доказательствами по уголовному делу нередко являются цифровые видео- и

¹⁰ Гришин А. Д. Совершенствование применения информационных технологий в досудебных стадиях уголовного судопроизводства // Вестник Московского университета МВД России. 2019. № 3. С. 120.

¹¹ Яшин А. В. Роль знаний о постпреступном поведении в практике предупреждения преступлений // Современные проблемы науки и образования. 2006. № 1. С. 110.

аудиозаписи, электронные документы, сообщения в социальных сетях. В отдельных случаях цифровые технологии могут являться способами фиксации следов преступления, которые существуют в нецифровой форме. Например, проводя осмотр места происшествия, следователь фиксирует некоторые виды следов, вещественных доказательств, показаний лиц на допросе с помощью специальных устройств: фотоаппаратов, видеокамер, диктофонов. Уровень технического прогресса достиг такой степени, что в настоящее время именно цифровые технологии способны наиболее точно зафиксировать следы преступлений.

Кроме того, на современном этапе достаточно развита технология искусственного распознавания личности, что способствует быстрой обработке большого объема информации, т. е. искусственный интеллект уже начинает входить в привычный обиход сотрудников правоохранительных органов. Представляется, что искусственному интеллекту следует доверить анализ материалов уголовного дела, что позволит сократить затраты рабочей силы сотрудников следственных органов. Интеллектуального помощника можно

запрограммировать таким образом, что он будет выдавать сведения об истечении процессуальных сроков или о допущенных технических ошибках при составлении тех или иных документов¹².

На основании изложенного представляется возможным сформулировать следующие варианты совершенствования применения информационных технологий в Следственном комитете России:

- расследование электронного уголовного дела с использованием специализированных программ и платформ;
- внедрение в следственную практику автоматизированных рабочих мест.

Полагаю, что это приведет к ускорению процедуры производства отдельных следственных действий.

Таким образом, разработка единой автоматизированной системы делопроизводства и электронного документооборота в Следственном комитете Российской Федерации существенно облегчила бы работу его подразделений и позволила бы рациональнее использовать как человеческие ресурсы, так и другие виды затрат.

Список литературы

1. Абдуллатипова К. А. Проблемы правового статуса Следственного комитета Российской Федерации // Закон и право. 2018. № 11. С. 39–41.
2. Багмет А. М. Проблемы обеспечения межведомственного электронного документооборота Следственного комитета Российской Федерации с

¹² Зазулин А. И. Функции цифровой информации и технологий в уголовном

процессе // Сибирское юридическое обозрение. 2020. № 1. С. 76.

федеральными государственными органами в сфере уголовного судопроизводства // Правопорядок: история, теория, практика. 2018. № 4. С. 45–49.

3. Бычков В. В. Электронный документооборот в следственной деятельности: проблемы и пути их решения / В. В. Бычков, С. Б. Вепрев // Правопорядок: история, теория, практика. 2018. № 4. С. 50–54.

4. Гришин А. Д. Совершенствование применения информационных технологий в досудебных стадиях уголовного судопроизводства // Вестник Московского университета МВД России. 2019. № 3. С. 119–122.

5. Зазулин А. И. Функции цифровой информации и технологий в уголовном процессе // Сибирское юридическое обозрение. 2020. № 1. С. 75–82.

6. Яшин А. В. История развития законодательства об уголовной ответственности за преступления против участников уголовного судопроизводства // Современное право. 2011. № 9. С. 156–158.

7. Яшин А. В. Криминологические особенности системы преступлений против участников уголовного судопроизводства // Пробелы в российском законодательстве. 2010. № 2. С. 237–239.

8. Яшин А. В. Некоторые проблемы предупреждения преступлений, совершаемых организованными группами или преступными сообществами // Наука. Общество. Государство. 2016. № 1. С. 61–67.

Farid Ya. Emirbekov

Student,

Ural State Law University

(Yekaterinburg, Russian Federation)

emirbekov.farid00@mail.ru

Scientific supervisor – M. V. Goncharov, PhD (Law), Associate Professor of the Department of Constitutional Law

PROBLEMS AND PROSPECTS OF USING ELECTRONIC DOCUMENT MANAGEMENT IN THE INVESTIGATIVE COMMITTEE OF THE RUSSIAN FEDERATION

Abstract: This article examines the problems of using electronic document management in the activities of the Investigative Committee of the Russian Federation for the investigation of criminal cases. The main functions of digital technologies used in the preparation of procedural and other investigative documents are analyzed. It is concluded that the use of information technologies and the development of a unified automated system of office management and electronic document management in the Investigative Committee of the Russian Federation can significantly increase the efficiency of investigative actions.

Keywords: investigative committee, criminal investigation, office management, electronic document management, automated information systems, artificial intelligence.

Научное издание

ТЕХНОЛОГИИ XXI ВЕКА В ЮРИСПРУДЕНЦИИ

Материалы
Третьей международной научно-практической конференции

(г. Екатеринбург, 21 мая 2021 года)

*Материалы публикуются в авторской редакции, авторы несут
ответственность за оригинальность и научно-теоретический уровень
публикуемого материала.*

Компьютерная вёрстка: Д. В. Бахтеев

Корректор: К. В. Бахтеева

Дизайн обложки: К. О. Хрущёва

Рисунок на обложке: Андрей tramdrey Негруль

Уральский государственный юридический университет
620137, г. Екатеринбург, ул. Комсомольская, 21
usla.ru

Кафедра криминалистики УрГЮУ
620137, г. Екатеринбург, ул. Комсомольская, 21
Тел.: +7 (343) 367-40-95

Проект CrimLib.info
Crimlib.info
ae@crimlib.info

Союз криминалистов и криминологов
crimescience.ru

Проект «Ритвус»
ritvus.ru

Электронное издание